

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-296490

(43)Date of publication of application : 29.10.1999

(51)Int.Cl.

G06F 15/16

G06F 9/44

G06F 15/00

G06F 17/30

(21)Application number : 10-102933

(71)Applicant : LAUREL INTELLIGENT
SYSTEMS:KK

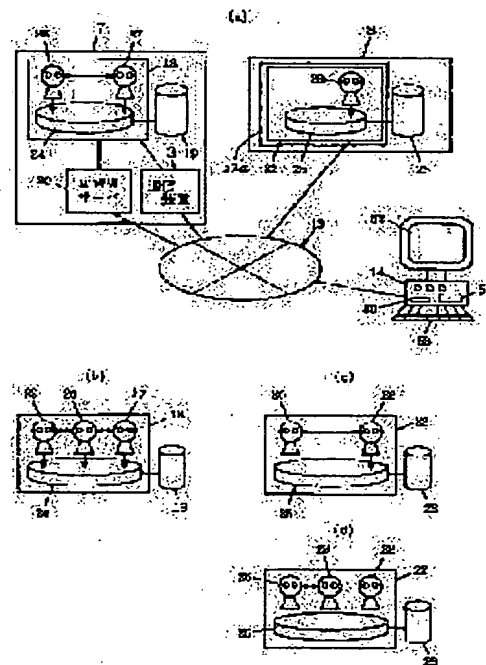
(22)Date of filing : 14.04.1998

(72)Inventor : TORIKAI MASAMICHI
FUJII MIKIO
TSUKAMOTO YUTAKA(54) MULTIAGENT SYSTEM, AGENT PRESENTING DEVICE RECORDING MEDIUM,
MULTIAGENT OPERATING METHOD AND MOBILE AGENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To execute a special job while maintaining neutrality when the special job that requires the neutrality is occurred in a multiagent system which is operated with agents cooperated with one another.

SOLUTION: When a user agent 26 wants to retrieve pay contents stored in a database 19 of a contents provider 7, a third party organization agent 29 of a third party organization 8 is called onto a place 24, and the third party organization agent 29 is provided with profile information of a user to be needed for retrieval. Then, the third organization agent 29 is made to perform the retrieval of the pay contents by propy.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-296490

(43) 公開日 平成11年(1999)10月29日

(51) Int.Cl. ⁶	識別記号	F I
G 0 6 F 15/16	4 3 0	G 0 6 F 15/16 4 3 0 Z
9/44	5 5 2	9/44 5 5 2
15/00	3 3 0	15/00 3 3 0 A
17/30		15/40 3 8 0 Z

審査請求 未請求 請求項の数12 O L (全 39 頁)

(21) 出願番号 特願平10-102933

(22) 出願日 平成10年(1998) 4 月14日

(71) 出願人 591234204

株式会社ローレルインテリジェントシステムズ
神奈川県横浜市青葉区美しが丘5丁目35番地の2

(72) 発明者 鳥飼 将迪

神奈川県横浜市青葉区美しが丘5丁目35番地の2 株式会社ローレルインテリジェントシステムズ内

(74) 代理人 弁理士 深見 久郎 (外2名)

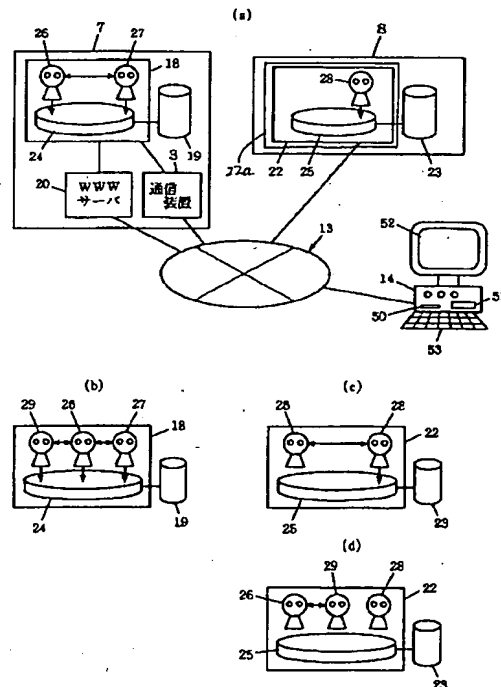
最終頁に続く

(54) 【発明の名称】 マルチエージェントシステム、エージェント提供装置、記録媒体、マルチエージェント運用方法、およびモバイルエージェントシステム

(57) 【要約】

【課題】 エージェント同士が協調して動作するマルチエージェントシステムにおいて中立性を要する特定の仕事が生じた場合にそれを中立性を保ちながら実行する。

【解決手段】 ユーザエージェント26がコンテンツ提供者7のデータベース19に格納されている有料コンテンツを検索したい場合には、第三者機関8の第三者機関エージェント29をブレース24上に呼出して、その第三者機関エージェント29に対し検索に必要となるユーザのプロフィール情報を提供し、その第三者機関エージェント29に有料コンテンツの検索の代理を行なってもらう。



【特許請求の範囲】

【請求項1】 それぞれに独立の知識を持つエージェント同士が協調して動作するマルチエージェントシステムであって、

当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が発生したことを判定する特定仕事判定手段を含み、

該特定仕事判定手段が前記特定の仕事が発生した旨の判定を行なった場合に、前記当事者双方に対し中立性を有する第三者エージェントが前記特定の仕事を代理して実行することを特徴とする、マルチエージェントシステム。

【請求項2】 前記第三者エージェントは、前記特定の仕事を処理するために設立された第三者機関により運用管理され、前記特定の仕事を前記のために開発されたエージェントであることを特徴とする、請求項1に記載のマルチエージェントシステム。

【請求項3】 前記特定仕事判定手段は、前記当事者のそれぞれの側のために働く当事者エージェント同士が協調して動作しているときに、該当事者エージェントでは自己の立場の方に有利となる利己的動作を行なうおそれのある場合に前記特定の仕事が発生した旨の判定を行なうことを特徴とする、請求項1または請求項2に記載のマルチエージェントシステム。

【請求項4】 有料コンテンツを格納しているコンテンツ格納手段をさらに含み、

前記当事者の一方は、前記コンテンツ格納手段内の格納コンテンツを提供するコンテンツ提供者であり、

前記当事者の他方は、前記コンテンツ提供者が提供するコンテンツ内に入手したいコンテンツがあるか否かの検索を希望するユーザであり、

前記特定仕事判定手段は、前記当事者エージェントのうちのユーザ側エージェントが前記コンテンツ格納手段に格納されている前記有料コンテンツの検索を希望した場合に前記特定の仕事が発生したことを判定することを特徴とする、請求項3に記載のマルチエージェントシステム。

【請求項5】 前記第三者エージェントは、依頼された仕事の実行を通して前記当事者の一方または双方に違法性があるかを監視する監視機能を有することを特徴とする、請求項1～請求項4のいずれかに記載のマルチエージェントシステム。

【請求項6】 請求項3に記載したマルチエージェントシステムに用いられる第三者エージェントを提供するためのエージェント提供装置であって、複数種類の第三者エージェントを格納しているエージェント格納手段と、

仕事を当事者エージェントに代わって第三者エージェントにより代理実行してもらいたい旨の依頼があった場合に、代理の対象となる前記当事者エージェントに応じた

種類の第三者エージェントを前記エージェント格納手段が格納している前記第三者エージェントの中から検索して提供するエージェント検索提供手段とを含むことを特徴とする、エージェント提供装置。

【請求項7】 それぞれに独立の知識を持つエージェント同士が協調して動作するマルチエージェントシステムに使用され、当事者の一方の側のために働くエージェントのプログラムを記録している記録媒体であって、コンピュータに、

当事者の他方のエージェントと打合せを行なう第1の打合せ手段と、

当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が発生した場合に、前記当事者双方に対し中立性を有する第三者エージェントと打合せを行なう第2の打合せ手段と、

前記特定の仕事を前記第三者エージェントに代理実行してもらうのに必要な情報を当該第三者エージェントに通知する必要情報通知手段と、して機能させるためのプログラムが記録された、コンピュータ読取可能な記録媒体。

【請求項8】 それぞれに独立の知識を持つエージェント同士を協調的に動作させるマルチエージェント運用方法であって、

当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が発生したことを判定する特定仕事判定ステップと、

前記当事者双方に対し中立性を有する第三者エージェントを調達する第三者エージェント調達ステップと、

前記特定仕事判定ステップにより前記特定の仕事が発生した旨の判定がなされた場合に、前記第三者エージェント調達ステップで調達された前記第三者エージェントが前記特定の仕事を実行する実行ステップとを含むことを特徴とする、マルチエージェント運用方法。

【請求項9】 エージェントがネットワーク上を移動して動作するモバイルエージェントシステムであって、ユーザと該ユーザの要求に応えるサービス業者とからなる当事者における前記ユーザ側のために働くユーザ側エージェントが、ネットワーク上を移動して動作するときのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアを含み、

前記ユーザ側エージェントは、秘密にしたい秘密データを秘密性が保持できる状態で前記知識として保有しており、該ユーザ側エージェントが移動して仕事を行なう際に、前記秘密データを使用する必要がある場合に、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し、該秘密保持用ワーキングエリア内で前記秘密データの秘密性を解除して前記仕事の実行を可能にすることを特徴とする、モバイルエージェントシステム。

【請求項10】 前記ユーザ側エージェントは、前記秘

密データを暗号化して保有しており、前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密データの復号化再生を可能にすることを特徴とする、請求項9に記載のモバイルエージェントシステム。

【請求項11】 前記ユーザ側エージェントは、前記秘密データの復号に用いられる復号鍵を保有しておらず、前記秘密保持用ワーキングエリアに移動した後前記秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密データの復号を可能にすることを特徴とする、請求項10に記載のモバイルエージェントシステム。 10

【請求項12】 前記秘密データは、前記ユーザの本人認証のための秘密鍵を含んでいることを特徴とする、請求項9～請求項11のいずれかに記載のモバイルエージェントシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば、ユーザの仕事を代行するエージェントと呼ばれる自律的なソフトウェアモジュールが動作するエージェントシステムに 20 関する。

【0002】

【従来の技術】この種のエージェントシステムにおいて、従来から知られているものに、たとえば、特開平9-179910号公報、特開平5-233574号公報、特開平5-233596号公報、特開平5-346910号公報、特開平5-151178号公報等に示すようなエージェント同士が協調して動作するマルチエージェントシステムがあった。

【0003】これらの従来のマルチエージェントシステムでは、それぞれに独立の知識を持ったエージェント同士が協調して仕事をしない、ある問題を効率的に解決できるように構成されていた。 30

【0004】

【発明が解決しようとする課題】ところが、たとえば、ユーザのために働くユーザ側エージェントとそのユーザの要求に応じて所定のサービスを提供するサービス業者側エージェントとが協調してある仕事をする場合に、ユーザ側エージェントと業者側エージェントとからなる当事者エージェントのみでは解決できない問題が生ずる場 40 合がある。

【0005】たとえば、サービス業者が有料コンテンツを提供する業者であって、ユーザ側エージェントが業者側エージェントと協調して有料コンテンツを検索して希望するコンテンツが見つければそのコンテンツを購入する仕事を想定してみる。ユーザ側エージェントがネットワーク上を移動してサービス業者側のプレースにまで行き、そのプレース上で業者側エージェントと打合せ(meeting)を行ない、有料コンテンツの検索の許可をもら 50 う。そしてユーザ側エージェントが有料コンテンツのデ

ータベースにアクセスして複数の有料コンテンツを検索してその中身を吟味し、希望するコンテンツがあるか否かを判断する。そしてもし希望するコンテンツがあれば、ユーザ側エージェントは所定の金額の料金を支払うための購入手続を行なった後希望するコンテンツをユーザ側に持ち帰る。

【0006】ところが、ユーザ側エージェントは、ユーザのために開発されユーザの利益となるように動作して仕事を行なうものであり、ユーザの命令に服従する性質のものである。その結果、ユーザがユーザ側エージェントに対し不正を働くように指令した場合やユーザ側エージェントを不正改造して不正を働くエージェントにするおそれが考えられる。そのようなユーザ側エージェントが前述した有料コンテンツを検索した場合に、希望するコンテンツが見つかったとしても業者側エージェントに対しては何ら希望するコンテンツがなかった旨の報告を行なって所定の料金を支払うための購入手続を何ら行なうことなく希望する有料コンテンツをこっそりユーザ側に持ち帰るという不正が発生するおそれがある。

【0007】そこで、このような不都合を防止するために、ユーザ側エージェントが直接コンテンツのデータベースにはアクセスできないようにし、ユーザ側エージェントに代わって業者側エージェントに有料コンテンツの検索を行なってもらふようにすることが考えられる。具体的には、たとえば、サービス業者側のプレース上でユーザ側エージェントと業者側エージェントとがmeetingして、ユーザの嗜好情報等のプロフィール情報や購入希望価格情報をユーザ側エージェントが業者側エージェントに通知し、それを知識として業者側エージェントがコンテンツのデータベースにアクセスして有料コンテンツを検索吟味し、ユーザが好むと思われるコンテンツを探し出してユーザ側エージェントにその結果を通知するようにすることが考えられる。

【0008】ところが、業者側のエージェントは、サービス業者側の利益のみを考慮して開発されて働くものであるために、サービス業者側の命令に服従する性質を有するものであり、その結果、コンテンツの検索結果ユーザが好むと思われるコンテンツがたとえなかったとしてもユーザ好みのコンテンツが多数あるという嘘の報告をユーザ側エージェントに通知する不都合が生ずるおそれがある。

【0009】つまり、ユーザ側エージェントや業者側エージェント等からなる当事者エージェントの場合には、互いの当事者の利益のためにのみ働く傾向があるために、自己の立場の方に有利となる利己的動作を行なうおそれがあり、当事者双方にとって中立性を要する特定の仕事が生じた場合にその特定の仕事を中立性を守りながら実行することができにくいという欠点が生ずる。

【0010】しかも、ユーザ側エージェントが知識として保有しているユーザのプロフィール情報は、たとえば

5

ユーザの種々の好みの情報からなる嗜好情報やユーザの年齢や職業あるいは年収等のような、ユーザが秘密にしたがる秘密情報を含んでいるのであり、サービス業者側のプレース上でユーザ側エージェントがそのような秘密情報を含んでいるプロフィール情報を業者側エージェントに通知した場合には、ユーザのプライバシーが損なわれるおそれが生じる。つまり、秘密情報を知得した業者側エージェントがその知得した知識に基づいて仕事を行なうてその知得した知識が不要になれば、その段階でユーザ側エージェントが知得した知識を破棄して消去するようにすれば、ユーザのプライバシーも保護されるのであるが、前述したように業者側エージェントは、サービス業者側の利益のために働くエージェントであるために、ユーザのプロフィール情報を知得すればそのようなプロフィール情報を後々までも記憶しておき、顧客管理やマーケティングに有効利用してサービス業者の利益のために活用する可能性が十分ある。なお、ユーザのプライバシーの問題は、秘密情報を知得して保有するユーザ側エージェントがサービス業者側のプレースに移動しただけでも脅かされるおそれがある。

【0011】本発明は、かかる実情に鑑み考え出されたものであり、その目的は、複数のエージェントが協調して動作する場合に、当事者がどうしても自己の利益を優先する傾向にあることに起因して生ずる種々の不都合を防止できるようにすることである。

【0012】

【課題を解決するための手段】請求項1に記載の本発明は、それぞれに独立の知識を持つエージェント同士が協調して動作するマルチエージェントシステムであって、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕が発生したことを判定する特定仕事判定手段を含み、該特定仕事判定手段が前記特定の仕が発生した旨の判定を行なった場合に、前記当事者双方に対し中立性を有する第三者エージェントが前記特定の仕事を代理して実行することを特徴とする。

【0013】請求項2に記載の本発明は、請求項1に記載の発明の構成に加えて、前記第三者エージェントは、前記特定の仕事を処理するために設立された第三者機関により運用管理され、前記特定の仕事をを行なうために開発されたエージェントであることを特徴とする。

【0014】請求項3に記載の本発明は、請求項1または請求項2に記載の発明の構成に加えて、前記特定仕事判定手段は、前記当事者のそれぞれの側のために働く当事者エージェント同士が協調して動作しているときに、該当事者エージェントでは自己の立場の方に有利となる利己的動作を行なうおそれのある場合に前記特定の仕が発生した旨の判定を行なうことを特徴とする。

【0015】請求項4に記載の本発明は、請求項3に記載の発明の構成に加えて、有料コンテンツを格納しているコンテンツ格納手段をさらに含み、前記当事者の一方

6

は、前記コンテンツ格納手段内の格納コンテンツを提供するコンテンツ提供者であり、前記当事者の他方は、前記コンテンツ提供者が提供するコンテンツ内に入手したいコンテンツがあるか否かの検索を希望するユーザであり、前記特定仕事判定手段は、前記当事者エージェントのうちのユーザ側エージェントが前記コンテンツ格納手段に格納されている前記有料コンテンツの検索を希望した場合に前記特定の仕が発生したことを判定することを特徴とする。

10 【0016】請求項5に記載の本発明は、請求項1～請求項4のいずれかに記載の発明の構成に加えて、前記第三者エージェントは、依頼された仕事の実行を通して前記当事者の一方または双方に違法性があるか否かを監視する監視機能を有することを特徴とする。

【0017】請求項6に記載の本発明は、請求項3に記載したマルチエージェントシステムに用いられる第三者エージェントを提供するためのエージェント提供装置であって、複数種類の第三者エージェントを格納しているエージェント格納手段と、仕事を当事者エージェントに代わって第三者エージェントにより代理実行してもらいたい旨の依頼があった場合に、代理の対象となる前記当事者エージェントに応じた種類の第三者エージェントを前記エージェント格納手段が格納している前記第三者エージェントの中から検索して提供するエージェント検索提供手段とを含むことを特徴とする。

【0018】請求項7に記載の本発明は、それぞれに独立の知識を持つエージェント同士が協調して動作するマルチエージェントシステムに使用され、当事者の一方の側のために働くエージェントのプログラムを記録している記録媒体であって、コンピュータに、当事者の他方のエージェントと打合せを行なう第1の打合せ手段と、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕が発生した場合に、前記当事者双方に対し中立性を有する第三者エージェントと打合せを行なう第2の打合せ手段と、前記特定の仕事を前記第三者エージェントに代理実行してもらうのに必要な情報を当該第三者エージェントに通知する必要情報通知手段と、して機能させるためのプログラムが記録された、コンピュータ読取可能な記録媒体。

40 【0019】請求項8に記載の本発明は、それぞれに独立の知識を持つエージェント同士を協調的に動作させるマルチエージェント運用方法であって、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕が発生したことを判定する特定仕事判定ステップと、前記当事者双方に対し中立性を有する第三者エージェントを調達する第三者エージェント調達ステップと、前記特定仕事判定ステップにより前記特定の仕が発生した旨の判定がなされた場合に、前記第三者エージェント調達ステップで調達された前記第三者エージェントが前記特定の仕事を実行する実行ステップとを含むことを特徴

50

とする。

【0020】請求項9に記載の本発明は、エージェントがネットワーク上を移動して動作するモバイルエージェントシステムであって、ユーザと該ユーザの要求に応えるサービス業者とからなる当事者における前記ユーザ側のために働くユーザ側エージェントが、ネットワーク上を移動して動作するときのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアを含み、前記ユーザ側エージェントは、秘密にしたい秘密データを秘密性が保持できる態様で前記知識として保有しており、該ユーザ側エージェントが移動して仕事を行なう際に、前記秘密データを使用する必要がある場合に、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し、該秘密保持用ワーキングエリア内で前記秘密データの秘密性を解除して前記仕事の実行を可能にすることを特徴とする。

【0021】請求項10に記載の本発明は、請求項9に記載の発明の構成に加えて、前記ユーザ側エージェントは、前記秘密データを暗号化して保有しており、前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密データの復号化再生を可能にすることを特徴とする。

【0022】請求項11に記載の本発明は、請求項10に記載の発明の構成に加えて、前記ユーザ側エージェントは、前記秘密データの復号に用いられる復号鍵を保有しておらず、前記秘密保持用ワーキングエリアに移動した後前記秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密データの復号を可能にすることを特徴とする。

【0023】請求項12に記載の本発明は、請求項9～請求項11のいずれかに記載の発明の構成に加えて、前記秘密データは、前記ユーザの本人認証のための秘密鍵を含んでいることを特徴とする。

【0024】

【発明の実施の形態】次に、本発明の実施の形態を図面に基づいて詳細に説明する。

【0025】図1は、情報の検索および配信システムの全体の概略を説明するための図である。図1を参照して、有線系メディアの一例としてのインターネット13に対し、ユーザ宅17のパーソナルコンピュータ（以下単にパソコンという）14とコンテンツ提供者7と第三者機関8と会員管理センター12と番組関連データ制作者11とコマーシャルメッセージ（以下単にCMという）制作者10と番組制作者9と放送局2とが接続可能に構成されている。

【0026】コンテンツ提供者7は、たとえば書籍情報や映画情報あるいは音楽情報、ニュース情報等の提供可能な情報を格納したデータベースを有しており、そのデータベース内の格納情報やその要約（アブストラクト）とを、インターネット13を経由してまたは無線系

メディアの一例としての放送局2からの衛星放送によりユーザ宅17のパソコン14に提供する。コンテンツ提供者7が提供可能なコンテンツの種類としては、その他に、たとえば課金のために暗号化された暗号化コンテンツデータやいわゆるネット家電を制御するための制御用プログラムデータ等が考えられる。

【0027】ユーザのパソコン14は、放送局2からたとえば衛星1を介して送信されてくる前述したアブストラクトデータを受信し、後述するユーザのエージェントによりそのアブストラクトを検索して取捨選択し、選択したアブストラクトデータをユーザに表示してユーザの選択指示を待つ。あるいは、ユーザにアブストラクト情報を表示する前に、そのアブストラクト情報の送信元であるコンテンツ提供者7にまで出向いて実際のコンテンツ情報にアクセスして内容を吟味し、本当にユーザが好むコンテンツであるか否かを確認し、確認後のアブストラクトをユーザに表示するようにしてもよい。

【0028】ユーザの指示またはユーザのエージェント独自の判断により、コンテンツを入手したい要望が発生すれば、コンテンツ提供者7は、その選択されたコンテンツ情報を放送局2に送信して所定の日時に放送してもらう。その放送予定日時と放送のチャンネル情報を放送局2から通知を受けたコンテンツ提供者7は、その放送日時とチャンネル情報をインターネット13を経由してユーザのパソコン14に送信する。

【0029】コンテンツ提供者7が提供するコンテンツ内に有料コンテンツが含まれている場合において、その有料コンテンツを販売する際には会員であるユーザのIDの確認が必要となる場合がある。その場合には、コンテンツ提供者7は、ユーザのID情報を要求し、そのID情報を会員管理センター12に送信し、IDの確認を行なってもらい、確認済のユーザのみに有料コンテンツの販売を行なう。

【0030】放送局2は、番組制作者9が制作した番組を入手し、その番組をアンテナ5、衛星1、アンテナ6を経由してユーザ宅17に向けて放送する。その放送される番組のためのCMがCM制作者10により制作され、そのCMデータがインターネット13を経由して放送局2にまで提供され、番組の合間にCMが挿入されて放送される。

【0031】放送局2から放送される番組を受信したユーザは、その番組を直接TV（テレビジョン）16により放映したり、パソコン14のCRTにより直接映し出して閲覧する場合もあるが、一旦VTR（ビデオテープレコーダ）15により録画し、後日その録画情報を再生して閲覧する場合がある。TV16は、このVTR15やパソコン14と連係して、ユーザが見たい場面だけを飛ばし飛ばし見るというイントロ再生機能や、複数のカメラ・アングルで撮影・放送された番組の場面切換をスムーズに実行できるようにする機能を有する。その機能

実現のために、高速なランダム・アクセスが可能なハード・ディスク装置や半導体メモリなどが内蔵されている。また放送局2側では、映像番組に関するインデックス情報を加えて放送する。ユーザ側では、受信した番組データをVTR15に記録させ、受信したインデックス情報をハード・ディスク装置などに蓄積する。このハード・ディスクは、VTR15から読出した映像データを一時的に蓄えるためにも使う。一般的に、VTRに蓄積した映像データは、検索から読出までに時間がかかる。しかし、VTR15から読出した映像データを一時的に

ハード・ディスクに蓄えれば、映像を再生している間にVTRの早送りを実行することができ、ユーザから見た必要な映像を取出すまでの待ち時間が短くなる。
【0032】このようにして、前述したいわゆるイントロ再生がスムーズに実行することができる。その結果、受信した番組内にCMが挿入されている場合には、ユーザにしてみれば、その贅肉に相当するCMのみをカットして番組だけを閲覧したがる傾向にあり、前述したイントロ再生機能によりそのCMカット閲覧が容易に実行可能となる。

【0033】そこで、このようなCMカット閲覧を防止する方法として、番組関連データをCMに重畳させて放送局2から放送する方法が考えられる。そのための番組関連データが番組関連データ制作者11により制作されて放送局2に転送される。この番組関連データとしては、番組の意見交換用のホームページのアドレスや、番組に出てくる専門用語の解説等が考えられる。

【0034】CM制作者10は、番組の合間に挿入されて放送局2から放送される一般的なCMばかりでなく、ユーザ(消費者)を多数の階層に分類してそれぞれの階層のみをターゲットにしたCMも作成する。この階層分けは、たとえば、性別、年齢別、学歴別、職業別、購買動向別等が考えられる。このようなターゲットを絞った多数のCMをCM制作者10が制作してデータベースに蓄積しておく。そして、ユーザのエージェントがそのCM制作者にまで出向いてデータベースを検索し、ユーザが好むと思われるCM情報を検索し、検索されたCM情報をインターネット13を経由してまたは放送局2からの放送により受信する。このようなユーザのエージェントによって検索されたCM情報も、番組関連データ制作者11が制作した番組関連データが重畳された状態でユーザに届けられるように構成されている。

【0035】図2は、マルチエージェントシステムの構成を示す説明図である。本実施の形態においては、ゼネラルマジック(General Magic)社が開発した通信用言語であるテレクリプトによる自律ソフトウェアとしてのエージェントを採用している。ユーザエージェント26は、モバイルエージェントで構成されている。モバイルエージェントとは、分散コンピューティング環境における移動性を備えたエージェントのことであり、ネット

ワークを介してエージェントがサーバーに転送・処理されること(リモート・プログラミング)が特徴となっている。モバイルエージェントが、テレクリプト・エンジンによって提供される共通動作環境であるプレースに移動して、そのプレース上で他のエージェントと協調して相互に動作して仕事を行ない問題を解決する。

【0036】ユーザのパソコン14内で動作しているユーザエージェントが、自己の判断でまたはユーザの操作指令に応じてコンテンツを検索する場合には、図2

(a)で示すように、コンテンツ提供者7のテレクリプト・エンジン18のプレース24に移動する。プレース24上に移動したユーザエージェント26は、プレース24に常駐している移動先エージェント27と打合せ(meeting)して、データベース19内のコンテンツを検索して希望するコンテンツを見つけ出してパソコン14にまで持ち帰る(送信する)。

【0037】なお、52はCRT、53はキーボード、50はICカード挿入口、51はフロッピーディスク(FD)挿入口、20はWWWサーバー、3は通信装置である。

【0038】一方、第三者機関8のテレクリプト・エンジン22のプレース25には、第三者機関常駐エージェント28が常駐している。データベース23内には、複数種類の第三者機関エージェントが機能別に分類されて格納されている。この第三者機関8は、当事者(たとえばユーザとそのユーザの要求に応じてサービスを提供するサービス業者)のみでは解決困難なまたは解決不可能な中立性を要する仕事が発生した場合に、そのような特定の仕事を当事者に代わって代理実行して解決するために設立された機関であり、官庁等の公な機関あるいは半公共的な機関によって構成するのが望ましい。なお、図中22aは、第三者機関8が運用管理するコンピュータである。

【0039】第三者機関8のデータベース23に格納されている各種第三者機関エージェントは、この第三者機関8によって運用管理されるものであり、前述した中立性を要する特定の仕事を中立性を守りながら実行して解決するために開発された専用のエージェントである。そして、ユーザエージェント26には、たとえば、オンラインショッピングするためのショッピングエージェント、ニュースソースからニュース記事を検索して必要なもののみを選び出すニュースフィルタリングエージェント、必要な電子メールのみを選び出す電子メールエージェント、ユーザの嗜好に合致した音楽情報や映画情報を検索するファイアフライ等の情報収集エージェントなど、種々の種類が存在する。そこでそのようなユーザエージェント26の仕事を代理実行する第三者エージェントの方も、ユーザエージェント26の種類に合せて機能別に複数種類用意しておく必要がある。

【0040】コンテンツ提供者7のプレース24に移

動したユーザエージェント26が移動先エージェント27と協調してデータベース19内のコンテンツを検索する際に、データベース19内の有料コンテンツを検索したい場合には、第三者機関常駐エージェント28と連絡をとり、データベース23から適した第三者機関エージェントを探し出してもらい、その第三者機関エージェントにコンテンツ提供者7のプレース24にまで出向してもらおう。

【0041】その状態が図2の(b)に示されている。出向してきた第三者機関エージェント29は、ユーザエージェント26とmeetingして、ユーザの好み等のプロフィール情報をユーザエージェント26から聞き出す。そして、コンテンツの検索に必要な知識を取得した状態で第三者機関エージェント29がデータベース19にアクセスして、ユーザエージェント26に代わってコンテンツの検索を行ないその検索結果をユーザエージェント26に知らせる。

【0042】第三者機関エージェント29がコンテンツを検索するためには、ユーザのプライバシーにかかわるような秘密情報(たとえばユーザの年収、学歴、貯蓄額等)をユーザコンテンツ26から教えてもらわなければならない場合は、コンテンツ提供者7のプレース24上でその秘密情報をユーザエージェント26が第三者機関エージェント29に通知すれば、その秘密情報がコンテンツ提供者7に漏れてしまうおそれがある。本実施の形態では、ユーザエージェント26は、前述したような秘密情報S1(図14参照)を暗号化して暗号化データとして保有しているために、ユーザエージェント26はコンテンツ提供者7のプレース24に移動しただけでは、その秘密情報S1がコンテンツ提供者7に知られてしまうことはない。しかし、コンテンツ提供者7のプレース24上において、第三者機関エージェント29が解読できるように暗号化秘密情報S1を復号化して平文の形で第三者機関エージェント29に教えた場合には、その平文の秘密情報S1がコンテンツ提供者7に知られる可能性が生ずる。

【0043】そこで、このような秘密情報S1を用いなければコンテンツが検索できない場合には、図2(c)に示すように、ユーザエージェント26が第三者機関8のテレスク립ト・エンジン22のプレース25にまで移動し、そこに常駐している第三者機関常駐エージェント28とmeetingして、最適な第三者機関エージェントを検索してもらい、その検索された第三者機関エージェント29とユーザエージェント26とがmeetingして、検索に必要な秘密情報S1を通知する(図2(d)参照)。

【0044】その後、ユーザエージェント26がコンテンツ提供者7のプレース24に復帰し、常駐エージェント27とmeetingして有料コンテンツを暗号化した形で第三者機関8のプレース25に転送してもらおう。そし

て転送されてきた有料コンテンツを復号化して第三者機関エージェント29がユーザエージェント26に代わってその有料コンテンツを検索して評価する。その評価結果をプレース24上のユーザエージェント26に通知する。このようにすれば、ユーザエージェント26が知識として保有している秘密情報S1がコンテンツ提供者7等に漏洩することが防止できる。なお、第三者機関8のプレース25上では、エージェント同士がいくらmeetingしても情報が外部に漏洩することが防止できるように構成されている。

【0045】図3は、ユーザのパソコン14の制御動作を示すフローチャートである。このユーザのパソコン14の制御回路は、図12に基づいて後述する。

【0046】図3を参照して、まずステップS(以下単にSという)1により、インターネット上のサイトを紹介する情報を受信したか否かの判断がなされる。この情報は、放送局2から衛星放送により放送されてユーザのパソコン14が受信したり、またはインターネット13経由で受信する。サイト紹介情報を受信していない場合にはS2に進み、記録対象コンテンツの放送日時になったか否かの判断がなされる。記録対象コンテンツとは、ユーザの入力指示によりVTR15等に記録する予定となっている番組等の放送局2から送られてくるコンテンツや、ユーザエージェントが独自の判断で記録予定にしている放送局2から送られてくるコンテンツのことである。記録対象コンテンツの放送日時になっていない場合にはS3に進み、放送番組のアブストラクトを受信したか否かの判断がなされる。前述したように、放送局2は、放送する番組の内容の要約(アブストラクト)を事前にユーザに向けて放送し、ユーザは、そのアブストラクト放送を受信してユーザエージェントに番組を録画記録させるかどうかを判断させる。放送番組のアブストラクトを受信していない場合にはS4に進み、ユーザからエージェントへの指示があったか否かの判断がなされる。

【0047】ユーザからエージェントへの指示がない場合には、S5に進み、コンテンツの再生指示があったか否かの判断がなされる。ない場合にはS6に進み、鍵SK1の送信要求があったか否かの判断がなされる。この鍵SK1は、前述した暗号化されている秘密情報S1を復号化するために用いられる鍵であり、後述するように第三者機関常駐エージェント28が必要に応じてユーザのパソコン14に対し送信要求を出すものである。SK1の要求がない場合にはS7に進み、ユーザエージェントから放送コンテンツの記録指示があったか否かの判断がなされる。ユーザのパソコン14内で動作しているユーザエージェントは、後述するように自己の判断に基づいて放送番組等の放送コンテンツを自動的に記録する指示をパソコン14に出す場合がある。

【0048】ユーザエージェントから放送コンテンツの

10

20

30

40

50

13

記録指示がない場合にはS 8に進み、放送日時とチャンネルを受信したか否かの判断がなされる。ユーザエージェントは、図9に基づいて後述するように、CM作成者10のプレイス25に移動してCMを検索し、希望するCMが見つければ、その希望するCMが放送局2から放送される日時とチャンネルをユーザのパソコン14に送信してくる。そのユーザエージェントからの放送日時とチャンネルが送信されてきたか否かがこのS 8により判断される。放送日時とチャンネルを受信していない場合にはS 9に進み、その他の処理がなされてS 1に戻る。

【0049】放送局2から放送されたサイト紹介情報あるいはインターネット13を経由して送信されてきたサイト紹介情報を受信すれば、S 1によりYESの判断がなされてS 10に進み、ユーザのパソコン14内で動作しているユーザエージェントにそのサイト紹介情報を知らせる処理がなされる。

【0050】S 2により、記録対象コンテンツの放送日時になったと判断された場合にはS 11に進み、放送されるチャンネル周波数にチューニングし、S 12により、放送コンテンツを受信してVTR 15に記録する処理がなされる。次にS 13に進み、記録したコンテンツがCMを含むか否かの判断がなされる。含まない場合にはS 1に戻るが、含む場合にはS 14に進み、編集時間があるか否かの判断がなされる。この編集時間とは、ユーザエージェントがCM制作者10のプレイス58に移動して検索して見つけ出したCMと放送局2が放送してVTR 15等に記録させた番組の合間に挿入されているCMとを差替える編集を行なうのに必要な時間のことである。

【0051】編集時間がある場合にはS 15に進み、対応する番組コンテンツのCM部分を検索したCMに取替える編集を行なった後S 1に戻る。編集時間がない場合にはS 16に進み、番組放映中にCM放送時間が来た瞬間ユーザエージェントが検索したCMに切換えて放映する制御を行なってS 1に戻る。

【0052】放送番組のアブストラクトが放送局2から放送されてそれを受信すればS 3によりYESの判断がなされてS 17に進み、ユーザエージェントにその受信したアブストラクトを知らせる処理がなされる。

【0053】ユーザがキーボード53やマウス等を操作してエージェントへの何らかの指示を行なえば、S 18に進み、パソコン14内で活動しているユーザエージェントにその指示を知らせる処理がなされる。

【0054】ユーザがキーボード53やマウス等を操作してコンテンツの再生指示を行なえばS 5によりYESの判断がなされてS 19に進み、再生の対象となるコンテンツが暗号化されたコンテンツであるか否かの判断がなされる。暗号化コンテンツの場合にはS 20によるコンテンツ再生処理を行なった後、S 21によるコンテンツの出力処理がなされてCRT 52やTV 16により放

14

映される。一方、暗号化コンテンツでない場合にはS 20の処理を行なうことなく直接S 21に進み、コンテンツ出力処理がなされる。S 26のコンテンツ再生処理の詳細は、図17に基づいて後述する。

【0055】鍵SK 1の送信要求があった場合にはS 6によりYESの判断がなされてS 22に進み、チャレンジデータCHを第三者機関常駐エージェント28へ送信する処理がなされる。このチャレンジデータCHは、パソコン14が生成した乱数等により構成される。第三者機関常駐エージェント28は、このチャレンジデータCHを受取り、第三者機関8の秘密鍵SK 3でそれを暗号化する処理すなわちE_{SK3}(CH)を算出してレスポンスデータRESとして返信する(SB 12, SB 23b 参照)。

【0056】このレスポンスデータRESを受信したパソコン14は、S 22aによりYESの判断がなされてS 22bに進み、受信したレスポンスデータRESを第三者機関8の公開鍵で復号化する処理すなわちD_{PK3}(RES)を演算し、その演算結果とS 22により送信したチャレンジデータCHとが一致するか否かの判断が行なわれる。正規の第三者機関8の第三者機関常駐エージェント28からSK 1の要求があったのであれば、CH=D_{PK3}(RES)となるはずであるために、その場合にはS 22cに進み、鍵SK 1を第三者機関8の公開鍵PK 3を用いて暗号化する演算すなわちE_{PK3}(SK 1)を算出して第三者機関常駐エージェント28へ送信する処理がなされる。一方、S 22bより一致しないと判断された場合にはS 22cの送信処理を行なうことなくS 1に戻る。

【0057】ユーザエージェントから放送コンテンツの記録指示があった場合にはS 23に進み、その指示のあった記録対象コンテンツの放送日時、チャンネルを記憶する処理がなされる。

【0058】ユーザエージェントから放送日時とチャンネルが送信されてくればS 8によりYESの判断がなされてS 24へ進み、その送信されてきた放送日時とチャンネルすなわち記録対象コンテンツの放送日時とチャンネルを記憶する処理がなされる。

【0059】図4～図6、図10は、ユーザエージェントの動作を示すフローチャートである。SA 1により、インターネット上のサイトの紹介情報を受取ったか否かの判断がなされ、受取っていない場合にはSA 2に進み、番組のアブストラクト情報を受取ったか否かの判断がなされ、受取っていない場合にはSA 3に進み、ユーザからの指示を受取ったか否かの判断がなされ、受取っていない場合にはSA 4に進み、ユーザエージェントが移動する時刻が来たか否かの判断がなされ、来ていない場合にはSA 5に進み、その他の処理を行なった後SA 1に戻る。

【0060】放送局2から放送されたサイト紹介情報を

15

受信した場合やインターネット13経由で送信されてきたサイト紹介情報を受取った場合には、SA6に進み、その情報内にコンテンツのアブストラクトが含まれているか否かの判断がなされる。コンテンツのアブストラクトが含まれている場合にはSA7に進み、そのアブストラクトとサイト紹介情報とでユーザエージェントが評価を行なう。この評価は、このユーザエージェントの持主であるユーザが好むサイトであるか否かあるいはユーザが好むコンテンツであるか否かを判断することである。ユーザエージェントは、たとえば後述する図14に示すようなユーザの嗜好情報等を含むプロフィール情報96を知識として保有しており、このプロフィール情報を活用して評価を行なう。

【0061】一方、コンテンツのアブストラクトが含まれていない場合にはSA8に進み、サイト紹介情報のみで評価を行なう。次にSA9に進み、評価が所定値以上であるか否かの判断がなされ、所定値以上でない場合にはSA1に戻る。一方所定値以上である場合にはSA10に進み、そのサイトのアドレスを移動先予定として登録した後SA1に戻る。

【0062】ユーザのパソコン14が放送番組のアブストラクトを受信してS17によりユーザエージェントに知らせた場合には、SA2によりYESの判断がなされてSA11に進み、その番組アブストラクトに基づいて番組の評価を行なう。この評価は、前述したように、ユーザのプロフィール情報96に基づいてユーザがどの程度好むかを判断して行なう。そして、SA12により、その評価が所定値以上であるか否かの判断がなされ、所定値以上でない場合にはSA1に戻るが、所定値以上の場合にはSA13に進み、推薦番組リストに登録する処理がなされる。この推薦番組リストに登録された番組がユーザに推薦番組として表示され、後述するようにユーザの指示を仰ぐ。ユーザがこの推薦番組の放送を受信して閲覧またはVTR15に録画する旨の指示を出せば、その指示された推薦番組が推薦番組リストから消去されることとなる。

【0063】SA14に進み、推薦番組リストに登録されている番組で放送日時が来るものがあるか否かの判断がなされ、ない場合にはSA1に戻る。この推薦番組リストに登録されているということは、前述したようにユーザに推薦する番組でありながら未だにユーザが閲覧するか破棄するかを指示を出していないものであり、そのようなユーザの指示がまだ出されていない推薦番組の放送日時が来てしまった場合には、SA15により、その推薦番組をユーザエージェントの自己判断で自動的に記録するか否かの判断を行なう。自動記録しないと判断された場合にはSA16により、推薦番組リストからその日時が来た番組を消去した後SA1に戻る。一方、自動記録すると判断された場合にはSA17に進み、その推薦番組リストに登録されている推薦番組を自動記録番組

16

リストの方に移し替えて登録する処理がなされる。

【0064】次にSA18に進み、パソコン14に対しコンテンツの記録指示を出す。その結果、前述したように、S7により、YESの判断がなされてS23により指示のあった記録対象コンテンツの放送日時、チャンネルが記録される。その結果、放送日時が現時点となるために、S2により即座にYESの判断がなされて、その放送日時が来た推薦番組を受信して記録する処理がS17以降で行なわれる。

【0065】次にSA19に進み、指示を出した番組コンテンツにCMがあるか否かの判断がなされる。ない場合にはSA16に進み、推薦番組リストから日時が来たものを消去する処理がなされる。つまり、推薦番組リストに登録されている推薦番組を受信して記録することとなったために、それ以降推薦番組リストに登録しておく必要がなくなるために、その記録することとなった推薦番組を推薦番組リストから消去するのである。

【0066】一方、SA19により、指示を出した番組コンテンツにCMがあると判断された場合にはSA20に進み、番組スポンサーに対応するCMを検索する処理がなされた後SA16に進む。このSA20のスポンサーに対応するCM検索処理は、後述する図10に基づいて説明する。

【0067】ユーザがユーザエージェントに対し指示を出した場合にはS18によりその指示がユーザエージェントに知らされ、その結果SA3によりYESの判断がなされてSA21に進む。SA21では、そのユーザからの指示が推薦番組リストの閲覧指示であるか否かの判断がなされ、閲覧指示の場合にはSA22に進み、推薦番組リストをCRT52またはTV16により表示する制御がなされる。一方、推薦番組リストの閲覧指示でなかった場合にはSA23に進み、自動記録番組リストの閲覧指示であるか否かの判断がなされる。SA23よりYESの判断がなされた場合にはSA24に進み、自動記録番組リストをCRT52またはTV16により表示させる制御がなされる。

【0068】自動記録番組リストの閲覧指示でなかった場合にはSA25に進み、コンテンツ検索結果の閲覧指示であるか否かの判断がなされる。ユーザエージェントがコンテンツを検索した場合には後述するようにその検索結果をパソコン14に送信するのであり、その検索結果の閲覧指示であった場合にはSA26により、コンテンツ検索結果をCRT52またはTV16により表示させる制御がなされる。

【0069】コンテンツ検索結果の閲覧指示でなかった場合にはSA27に進み、推薦番組の記録指示であるか否かの判断がなされる。SA22により表示された推薦番組を閲覧したユーザがその推薦番組の中から記録して閲覧したいものがあつた場合にはその記録希望の推薦番組の記録指示を出す。その結果SA27によりYESの

10

20

30

40

50

17

判断がなされてSA29に進み、その指示された推薦番組コンテンツの記録指示をパソコン14に出す処理がなされる。その結果、パソコン14では、S7によりYESの判断が行なわれてS23により、その指示された記録対象コンテンツの放送日時、チャンネルを記録する処理がなされ、その結果、S2により、その記憶した記録対象コンテンツの放送日時になった場合にS11以降のコンテンツの記録処理が実行されることとなる。

【0070】次にSA30に進み、指示を出した番組を推薦番組リストから消去する処理がなされた後SA19に進む。

【0071】推薦番組記録指示でなかった場合にはSA28に進み、ユーザエージェントがその他の処理を実行してSA1に戻る。

【0072】SA3によりNOの判断がなされた場合にはSA4に進み、移動時刻が来たか否かの判断がなされる。この移動時刻とは、ユーザエージェントがネットワークを介してインターネット上のサイトに移動し、コンテンツ等の検索を実行する時刻のことであり、予め設定されている時刻である。未だに移動時刻が来ていない場合にはSA5に進み、その他の処理を実行した後SA1に戻る。一方、移動時刻が来た場合にはSA5aに進み、エージェント移動処理を実行した後SA1に戻る。このエージェント移動処理は、図5、図6に示されている。

【0073】次に、図5、図6に基づいて、エージェント移動処理のフローチャートを説明する。SA31により、ユーザエージェントを移動させる処理を行なう。このユーザエージェントの移動先は、前述したSA10により移動先予定として登録されたアドレスにより特定される。このユーザエージェントの移動は、実際には、ユーザのパソコン14内のユーザエージェントと全く同じユーザエージェント（クローン）を複製してそれを移動先に転送する処理である。

【0074】次にSA32に進み、移動先のプレースに常駐している移動先エージェント27とmeeting（打合せ）して、種々の必要な情報交換を行なう。次にSA33に進み、そのmeetingの結果に基づいて、データベース19内に無料コンテンツがあるか否かの判断を行ない、無料コンテンツがある場合にはSA34に進み、その無料コンテンツを検索する処理を行ない、SA35によりその検索が完了したか否かの判断を行ない、完了するまで無料コンテンツの検索処理を続行する。そして完了した段階でSA36に進む。一方、無料コンテンツがないと判断された場合には直接SA36に進む。

【0075】SA36では、データベース19内に有料コンテンツがあるか否かの判断がなされ、ない場合にはSA38に進み、移動先エージェント27とmeetingして、選択したコンテンツのパソコン14への送信指令を出してもらう。次にSA39に進み、検索結果をパソ

18

コン14に送信する処理を行ない、SA40に進み、移動が終了したか否かの判断がなされる。SA10により登録された移動先予定をすべて移動した場合には移動終了と判断されてSA40aに進み、自分自身を消去して終了する。一方、SA40により移動終了でないと判断された場合には再びSA31に進み、次の移動予定のアドレスにユーザエージェントが移動して前述と同様の処理を行なう。

【0076】一方、SA36により有料コンテンツがあると判断された場合にはSA37に進み、その有料コンテンツをコンテンツのアブストラクトにより検索する処理を行なう。そしてSA41によりその検索が完了するまでその検索を続行する。検索が完了した段階でSA42に進み、有料コンテンツ内に、所定料金を超える高額有料コンテンツがあるか否かの判断がなされ、ない場合にはSA39に進み、有料コンテンツのアブストラクトによる検索結果をパソコン14へ送信する。高額有料コンテンツがある場合にはSA43に進み、その高額有料コンテンツ内に入手したいものがあるか否かの判断が行なわれる。この判断は、高額有料コンテンツの前述したアブストラクトにより判断する。入手したいものがない場合にはSA39に進むが、入手したいものがある場合にはSA44に進む。

【0077】以上の説明のように、高額有料コンテンツでない低額有料コンテンツに対しては、そのコンテンツのアブストラクトのみを検索してその検索結果をパソコン14へ送信し、ユーザの指示を仰ぐ。一方、高額有料コンテンツ内に入手したいものがある場合には、SA44により、その入手希望高額コンテンツの検索に秘密情報（S1）が必要であるか否かの判断がなされる。必要でない場合にはSA45に進み、移動先エージェント27に自己のエージェントの種類を知らせて最寄りの第三者機関エージェントに出向依頼を行なう処理がなされる。移動先エージェント27は、この依頼を受けて、最寄りの第三者機関8の第三者機関常駐エージェント28と交信し、ユーザエージェント26の種類に応じた最適な種類の第三者機関エージェントの出向（派遣）を依頼する。その依頼を受けて、第三者機関エージェントが移動先であるたとえばコンテンツ提供者7のプレース24に出向してくれば、SA46により、YESの判断がなされてSA64へ進む。

【0078】SA64では、出向してきた第三者機関エージェント29とmeeting（打合せ）して入手希望高額コンテンツの検索の代理を行なってもらうよう依頼する（図2（b）参照）。すると、後述するように、第三者機関エージェント29は、必要なプロフィール情報96をユーザエージェント26から聞き出してそれに基づいてデータベース19にアクセスして入手希望高額コンテンツの検索を行ない、ユーザエージェント26の持主であるユーザが好むであろうと予想される高額コンテンツ

19

を検索してその評価を行なう。次にSA66により、ユーザエージェント26が第三者機関エージェント29に対し検索結果の評価を知らせてもらう。

【0079】次にSA67に進み、検索された有料コンテンツを購入するか否かの判断をユーザエージェント26が行なう。購入しない場合にはSA39に進むが、購入する場合にはSA68に進み、移動先エージェント27とmeetingして、オーダ情報OIと支払い指示PIとの暗号化情報E_{PK3}(OI)、E_{PK3}(PI)を受取る。このオーダ情報OIは、購入を希望する有料コンテンツの種類を特定するコンテンツNOと購入するという意思表示情報等である。また支払い指示PIとは、たとえばクレジットかあるいは電子キャッシュか等の支払い方法とその支払い金額情報である。それらの情報OIとPIとを第三者機関8の公開鍵P_{K3}で暗号化した情報を移動先エージェント27からユーザエージェント26が受取る。

【0080】次にSA69に進み、その受取った情報とともに第三者機関8のプレース25へ移動する。次にSA70により、第三者機関常駐エージェント28とmeetingして(図2(c)参照)、ユーザの秘密鍵SKUをユーザの鍵SK1で暗号化した暗号化秘密鍵E_{SK1}(SKU)と、前述したE_{PK3}(OI)、E_{PK3}(PI)とを第三者機関常駐エージェント28に知らせるとともに、秘密情報SIの復号鍵SK1をユーザのパソコン14から取り寄せてもらう依頼を行なう。

【0081】第三者機関常駐エージェント28は、ユーザのパソコン14からSK1を受取ってその鍵を用いて復号化処理を行ない、SKU、OI、PIを再生し、OI、PIについてハッシュ化してオーダ情報ダイジェストOI'と支払い指示ダイジェストP'を生成し、その両ダイジェストを合せた状態でユーザの秘密鍵SKUで暗号化し、そのE_{SKU}(OI',PI')を生成する。SA71では、ユーザエージェント26は、そのE_{SKU}(OI',PI')を受取り移動先であるコンテンツ提供者7のプレース24に復帰する。次にSA72により、移動先エージェント27とmeetingして、E_{SKU}(OI',PI')を通知するとともに、選択したコンテンツのパソコン14への送信指令を出してもらう依頼を行なう。そしてその後SA39へ進む。

【0082】前述したユーザの秘密鍵SKUは、たとえばRSA公開鍵暗号方式に用いられる秘密鍵のことであり、このユーザの秘密鍵が、エレクトリックコマースにおける本人認証用のデジタル署名等に用いられる。なお、SKUの秘密鍵やそれに対応する公開鍵を用いた暗号化や復号化のアルゴリズムは、RSA公開鍵暗号方式のアルゴリズムの代わりに、いわゆる楕円曲線暗号のアルゴリズムを用いてもよい。

【0083】次に、前述したSA44により、入手希望高額コンテンツの検索に秘密情報SIが必要であると判

20

断された場合にはSA47に進み、ユーザ認証が必要であるか否かの判断がなされる。コンテンツ提供者の中には、高額コンテンツの検索を希望するユーザエージェントに対し、本人認証を要求する場合がある。すなわち、検索対象となるコンテンツの料金が高額であるために、閲覧希望を出したユーザエージェントとその持主であるユーザが本当に本人自身であるか否かを確かめ、他人によるなりすましを防止したいと希望するコンテンツ提供者が存在する。そのような場合には、SA47により、ユーザ認証が必要であると判断され、SA48に進み、認証対象メッセージNMを暗号化した暗号化認証対象メッセージE_{PK3}(NM)をユーザエージェント26が移動先エージェント27から受取る。

【0084】このPK3は、前述したように、第三者機関8の公開鍵である。そしてSA49に進み、最寄りの第三者機関8へユーザエージェント26が移動し、第三者機関常駐エージェント28とmeetingして最適な第三者機関エージェントを検索してもらうとともに、秘密情報の復号鍵SK1をパソコン14から取り寄せてもらう依頼を行なう。次にSA51に進み、検索された第三者機関エージェントとmeetingし、必要な暗号化秘密情報E_{SK1}(SI)をその第三者機関エージェント29に通知する。次にSA52に進み、ユーザ認証が必要であったか否かの判断がなされ、必要であった場合にはSA53に進み、第三者機関エージェントからE_{SKU}(NM)を受取った後SA54へ進む。

【0085】第三者機関エージェント29は、後述するように、E_{PK3}(NM)を第三者機関の秘密鍵SK3で復号化して再生されたNMをユーザの秘密鍵SKUで暗号化した情報すなわちE_{SKU}(NM)を生成する。ユーザエージェント26は、第三者機関エージェント29とmeetingして、そのE_{SKU}(NM)を受取るのである。なおこの認証対象メッセージNMは、たとえば、移動先エージェント27が生成した乱数等である。

【0086】次にSA54では、たとえばコンテンツ提供者7のプレース24等の移動先へ復帰する処理がなされ、SA55に進み、移動先エージェント27とmeetingして、暗号化された入手希望高額コンテンツE_{PK3}(KC)を第三者機関8に転送してもらう依頼を行なう。

【0087】第三者機関エージェント29は、E_{PK3}(KC)を復号化して再生された入手希望高額コンテンツKCを検索して評価を行ない、その検索結果の評価を第三者機関8の秘密鍵であるSK3により暗号化し、その暗号化データであるE_{SK3}(HK)を移動先のプレース24上のユーザエージェント26へ転送する。すると、SA56によりYESの判断がなされてSA57に進み、その受取ったデータを第三者機関の公開鍵P_{K3}で復号化する処理すなわちD_{PK3}{E_{SK3}(HK)}を演算して、評価HKを再生する処理を行なう。

【0088】次にSA58へ進み、再生された評価HKに基づいて有料コンテンツを購入するか否かの判断が行なわれ、購入しない場合にはSA59により処理完了した旨を第三者機関8へ通知した後SA39へ進む。一方、購入する場合にはSA60へ進み、移動先エージェント27とmeetingして、オーダ情報OIと支払い指示PIとの暗号情報E_{PK3}(OI)、E_{PK3}(PI)を第三者機関8へ転送してもらう依頼を行なう。第三者機関常駐エージェント28は、前述と同様に、E_{SKU}(OI', PI')を生成し、それを移動先のユーザエージェント26へ送信する。その結果、SA61によりYESの判断がなされてSA62へ進み、移動先エージェント27とmeetingして、選択したコンテンツの送信指令を行なってもらうよう依頼する。次にSA63に進み、処理完了した旨を第三者機関8へ通知した後、SA39へ進む。

【0089】前述したE_{SKU}(OI', PI')が、いわゆるSET(Secure Electronic Transaction)で規定されているオーダ情報と支払い指示とに対するユーザの二重署名である。

【0090】図7は、第三者機関常駐エージェント28の動作を示すフローチャートである。SB1により、出向依頼(派遣依頼)があったか否かの判断がなされ、ない場合にはSB2に進み、ユーザエージェント26が第三者機関8のプレース25に来たか否かの判断がなされ、来ていない場合にはSB3に進み、ユーザエージェント26から処理完了の旨の通知があったか否かの判断がなされ、ない場合にはSB4へ進み、移動先エージェント27からE_{PK3}(OI)、E_{PK3}(PI)が送信されてきたか否かの判断がなされ、送信されてきていない場合にはSB1へ戻る。

【0091】ユーザエージェント26が第三者機関エージェントの出向依頼を移動先エージェント27に対し行ない移動先エージェント27が出向依頼があった旨と出向依頼をしたユーザエージェント26の種類(たとえばオーソリティ情報)を第三者機関常駐エージェント28に通知すれば、SB5に進み、第三者機関常駐エージェント28は、通知されたエージェントの種類に基づいてデータベース23にアクセスして第三者機関エージェントを検索する処理を行なう。そして、ユーザエージェント26の種類に合致する最適な第三者機関エージェント29を検索してSB6により、その検索された第三者機関エージェント29に出向指令を出す処理がなされて、SB1に戻る。

【0092】前述したSA49またはSA69により、ユーザエージェント26が第三者機関8のプレース25に来た場合には、SB2によりYESの判断がなされてSB7に進み、ユーザエージェント26とmeetingする。そして必要な種々の情報交換を行ない、SB8に進み、ユーザエージェント29が来た目的が、第三者機関

エージェント29への仕事依頼のためなのか否かの判断が行なわれる。ユーザエージェント26がSA49に基づいて第三者機関8のプレース25に来たのであれば、SB8によりYESの判断がなされてSB9に進み、第三者機関エージェント29を検索する処理がなされる。

【0093】次にSB10に進み、ユーザエージェント26の出所すなわちパソコン14を呼出し、秘密情報SIの暗号化データを復号化するための鍵SK1を要求する処理がなされる。この要求を受けたパソコンは、前述したように、SK1を要求してきた第三者機関8が本当に正規の第三者機関であるか否かの認証を行なうために、乱数を発生させてその乱数をチャレンジデータCHとして返信する。そのチャレンジデータCHを受信した第三者機関常駐エージェントは、SB11によりYESの判断がなされてSB12に進み、E_{SK3}(CH)をレスポンスデータRESとしてパソコン14へ送信する。

【0094】パソコン14側では、前述したように、その送信されてきたレスポンスデータRESを第三者機関の公開鍵PK3で復号化して先ほどのチャレンジデータCHと一致するか否かの判断が行なわれ、一致する場合にのみ鍵SK1を第三者機関の公開鍵PK3で暗号化したE_{PK3}(SK1)を送信する。それを受信した第三者機関常駐エージェントでは、SB14によりYESの判断がなされ、SB15に進み、その受信データを第三者機関8の秘密鍵で復号化する処理すなわちD_{SK3}{E_{PK3}(SK1)}を演算してSK1を再生する。次にSB16に進み、検索された第三者機関エージェント29にそのSK1を通知する処理がなされてSB17へ進む。

【0095】SB17では、ユーザエージェント26が移動先すなわちコンテンツ提供者7のプレース24へ復帰したか否かの判断が行なわれ、復帰するまで待機する処理が行なわれる。第三者機関8のプレース25に移動してきたユーザエージェント26は、前述したSA50～SA53の処理を行なった後、移動先へ復帰するのであり(SA54参照)、移動先であるコンテンツ提供者7のプレース24へユーザエージェント26が復帰した段階でSB18へ進み、ユーザエージェント26のクローンを消去する処理がなされる。これにより、仕事を終了したユーザエージェント26は、第三者機関エージェント28のプレース25上には存在しない状態となる。次にSB19に進み、第三者機関常駐エージェント28は、第三者機関エージェント29とmeetingして、ユーザの秘密鍵であるSKUを開き出す処理を行なった後、制御がSB1へ戻る。

【0096】ユーザエージェント26が前述したSA69に基づいて第三者機関エージェント8のプレース25に来た場合には、SB8によりNOの判断がなされてSB20以降の処理がなされる。つまり、ユーザエージェント26がSA69に従って第三者機関8に来るとい

ことは、有料コンテンツの購入手続を行なうために必要な処理を秘密情報の漏洩を防止しながら行なうためである。そのような場合には、第三者機関常駐エージェント28は、まずSB20により、やってきたユーザエージェント26から、E_{SK1} (SKU)、E_{PK3} (OI)、E_{PK3} (PI)を受取る。次にSB21により、オーダ情報OIと支払い指示PIを再生する処理、すなわち、D_{SK3} { E_{PK3} (OI) }, D_{SK3} { E_{PK3} (PI) }を演算する。

【0097】次にSB22に進み、OIとPIとをハッシュ化して両者のダイジェストOI', PI'を算出する処理がなされる。次にSB23へ進み、ユーザエージェント26の出所すなわちパソコン14に対し、SK1を要求する処理が行なわれる。

【0098】ユーザのパソコン14が前述と同様にチャレンジデータCHを送信してくれば、SB23aによりYESの判断がなされてSB23bに進み、受信したチャレンジデータCHを第三者機関8の秘密鍵SK3で暗号化したE_{SK3} (CH)をレスポンスデータRESとしてパソコン14へ送信する処理がなされる。パソコン14では、前述したようにE_{SK3} (CH)に基づいて第三者機関8の認証を行ない、認証結果正しいと判断された場合にはE_{PK3} (SK1)を送信する。第三者機関常駐エージェント28がそれを受信すれば、SB25へ進み、D_{SK3} { E_{PK3} (SK1) }が演算され、SK1が再生される。

【0099】次にSB26へ進み、D_{SK1} { E_{SK1} (SKU) }を演算してユーザの秘密鍵SKUを再生する処理が行なわれる。次にSB27へ進み、E_{SKU} (OI', PI')を演算してユーザエージェント26に通知する処理が行なわれる。このE_{SKU} (OI', PI')がオーダ情報と支払い指示に対するユーザの二重署名となる。3次にSB27aに進み、ユーザエージェントが復帰したか否かの判断がなされる。ユーザエージェント26は、前述したように、SA70の処理を行なった後移動先であるコンテンツ提供者7のプレース24に復帰するのであり(SA71参照)、ユーザエージェント26が復帰した段階でSB27bに進み、ユーザエージェントのクローンを消去する処理がなされた後SB1へ戻る。

【0100】図8は、第三者機関エージェント29の動作を示すフローチャートである。SC1により出向指令があったか否かの判断がなされ、ない場合にはSC2に進み、E_{SK1} (SI)を通知されたか否かの判断がなされ、通知されていない場合にはSC1へ戻る。

【0101】このSC1、SC2のループの巡回途中で、第三者機関常駐エージェント28から出向指令を任命されれば(SB6参照)、SC1によりYESの判断がなされてSC3へ進み、たとえばコンテンツ提供者7のプレース24等の移動先に移動する処理が行なわれ

る。この移動処理は、具体的には、第三者機関エージェント29をデータベース23内に残したままその第三者機関エージェント29のクローンを移動先のプレース24へ転送する処理である。次にSC4に進み、移動先のプレース24上において、ユーザエージェント26とmeetingして、入手希望高額コンテンツを通知してもらうとともに、必要なユーザのプロフィール情報96(図14参照)を教えてもらう処理が行なわれる(SA64参照)。このユーザエージェント26から教えてもらうユーザのプロフィール情報96は、公表可能情報NSI(図13参照)に限定される。これは、秘密情報の漏洩が防止可能な第三者機関8のプレース25上でのユーザプロフィール情報のやり取りではなく、情報提供者7のプレース24上でのユーザプロフィール情報のやり取りであるために、秘密性が保持できず、そのために秘密性を保持する必要のない公表可能情報NSIに限定されるのである。

【0102】次にSC5に進み、入手希望高額コンテンツの評価を行なう処理がなされる。この評価は、教えてもらったユーザプロフィール情報96に基づいて、ユーザが好むであろうと推測される度合いを数値化して行なう。次にSC6に進み、入手希望高額コンテンツは違法なコンテンツであるか否かの判断がなされる。違法なコンテンツとは、たとえば、麻薬の密輸ルートに関するコンテンツや拳銃の入手経路に関するコンテンツ等の刑法に違反するようなコンテンツである。また、風俗営業法に違反するようなコンテンツも違法コンテンツに含めてもよい。

【0103】違法なコンテンツでないと判断された場合にはSC10へ進み、第三者機関エージェント29が自分自身を消去して終了する。一方、違法なコンテンツであると判断された場合にはSC7へ進み、違法のため購入できない旨の評価をユーザエージェント26に知らせ、SC8により、違法である旨の通報を警察に行なう。次にSC9へ進み、違法コンテンツを第三者機関8に持ち帰り証拠として保管する処理を行なった後SC10へ進む。

【0104】SC1、SC2のループの巡回途中で、ユーザエージェント26により、ユーザのプロフィール情報のうちの秘密情報SIを暗号化した情報であるE_{SK1} (SI)が通知された場合(SA51参照)には、SC2によりYESの判断がなされてSC11に進み、第三者機関常駐エージェント28とmeetingして、復号化するための鍵SK1を教えてもらう処理がなされる。次にSC12へ進み、D_{SK1} { E_{SK1} (SI) }を演算して秘密情報SIを再生して記憶する処理がなされる。

【0105】次にSC18へ進み、ユーザ認証が必要であるか否かの判断がなされ、必要でない場合にはSC15へ直接進むが、必要な場合にはSC14へ進む。SC14では、E_{SKU} (NM)を演算してユーザエージェン

ト26へ知らせる処理がなされる。このNMは、移動先エージェント27からユーザエージェント26が受取った認証対象メッセージであり、第三者機関の公開鍵で暗号化された暗号化情報として受取る(SA48参照)。そしてこの暗号化認証対象メッセージがユーザエージェント26より第三者機関8のプレース25に持込まれ、第三者機関常駐エージェント28により復号化されて再生された認証対象メッセージNMが第三者機関エージェント29に知らされる。第三者機関エージェント29は、その通知されたNMとSC12により再生されたS1の中に含まれているユーザの秘密鍵SKU(図14参照)に基づいて、ESKU(NM)を演算してユーザに知らせる。このESKU(NM)が、ユーザの本人認証用のデータとなり、ユーザエージェント26はそれを受取り(SA53参照)、移動先のプレース24へ復帰して(SA54参照)、そのプレース24上の移動先エージェント27にESKU(NM)を知らせる。

【0106】次にSC15へ進み、EPK3(KC)を受信したか否かの判断がなされ、受信するまで待機する。ESKU(NM)を移動先のプレース24へ持ち帰ったユーザエージェント26は、移動先エージェント27に対し入手希望高額コンテンツKCを暗号化したEPK3(KC)を転送してもらう依頼を行なう(SA55参照)。これを受けた移動先エージェント27は、EPK3(KC)を第三者機関8の第三者機関エージェント28へ送信する。その送信されてきたEPK3(KC)を受信すればSC16へ進み、DPK3{EPK3(KC)}を演算してKCを再生する処理が行なわれる。次にSC17へ進み、その入手希望高額コンテンツKCの評価を行なう処理がなされる。

【0107】次にSC18へ進み、入手希望コンテンツは違法なコンテンツであるか否かの判断がなされる。この判断は、前述したSC6と同様に行なわれる。そして違法なコンテンツである場合にはSC7へ進むが、違法なコンテンツでない場合にはSC19へ進み、入手希望高額コンテンツKCの評価HKに対し第三者機関8の秘密鍵SK3で暗号化したデータすなわちESK3(HK)を演算し、SC20により、その演算結果を移動先のプレース24上にいるユーザエージェント26に送信する処理がなされた後SC10へ進む。

【0108】図9は、CM制作者10におけるエージェントの動作を説明するための説明図である。CM制作者10のテレスク립ト・エンジン57内のCMプレース58には、常駐エージェント59が存在する。図中、56はCM制作者10が制作した多数のCMを格納しているデータベース、54はWWWサーバー、55は情報処理コンピュータである。

【0109】ユーザのパソコン14内で動作しているユーザエージェントは、必要に応じてインターネット13を経由してCM制作者10のCMプレース58に移動す

る。そのCMプレース58上において、ユーザエージェント26と常駐エージェント59とがmeetingし、両者協調してユーザが好むと思われるCMを検索する。

【0110】図10は、図4のSA20に示したスポンサーに対応するCM検索の具体的な動作を示すユーザエージェントのフローチャートである。SA73により、ユーザエージェントがパソコン14からCMプレース58へ移動する。この移動は、パソコン14内のユーザエージェント26を複製してクローンを作成し、そのクローンをユーザエージェント26としてCMプレース58へ派遣することにより行なわれる。次にSA74へ進み、自分のクローンが既にCMプレース58に駐在しているか否かの判断がなされ、既に駐在している場合にはSA73に戻り、次のCM制作者10のCMプレース58へ移動する。

【0111】このSA73、SA74により、ユーザエージェント26は、自分のクローンが駐在していないCMプレース58を見つけ出してそこに移動することとなる。自分のクローンが駐在していないCMプレースを見つけ出した場合には、SA75に進み、データベース56にアクセスしてCMを検索する処理が行なわれる。次にSA76へ進み、希望するCMがあったか否かの判断がなされ、ない場合にはSA81へ進むが、あった場合にはSA77に進む。SA77では、希望するCMを電波メディア(無線系メディア)を利用してユーザ宅17にまで送信するかまたはインターネット等の有線系メディアを利用して送信するか判断が行なわれる。電波メディアを利用しないと判断された場合にはSA78へ進み、希望するCMをインターネット13経由でパソコン14に送信する処理がなされる。

【0112】一方、電波メディアを利用する場合にはSA79へ進み、常駐エージェント59とmeetingして、希望するCMの放送日時とチャンネルを教してもらう処理がなされる。次にSA80へ進み、放送日時とチャンネルと記録指示をインターネット13を経由してパソコン14へ送信する処理がなされる。

【0113】次にSA81へ進み、ユーザエージェント26がこのCMプレース58に駐在するか否かの判断がなされる。駐在しない場合にはSA86へ進み、移動が終了したか否かの判断がなされ、移動予定となっているCM作成者の中にまだ移動していないところがある場合にはSA73に戻り、次の移動先へ移動する。一方、移動予定となっているすべてのCM作成者10を移動し終わった場合にはSA78へ進み、ユーザエージェント26がユーザのパソコン14へ復帰する処理がなされて制御が終了する。

【0114】一方、ユーザエージェント26がこのCMプレース58に駐在すると判断した場合にはSA82へ進み、自分のクローンを作りそれを移動先予定となっている他のCM作成者10のCMプレースに移動させる処

理がなされる。次にSA83へ進み、CMプレース58に駐在することとなったユーザエージェント26が、常駐エージェント59とmeetingして、新たなCM作成があったか否かの判断がなされる。CM制作者10が新たなCMを制作してデータベース56に記憶させれば新たなCMが制作された旨を常駐エージェント59がCMプレース58に駐在しているユーザエージェント26に知らせるのであり、その知らせがあれば、SA83によりYESの判断がなされてSA88へ進む。

【0115】SA88では、CMプレース58に駐在しているユーザエージェント26がその新たなCMを検索して評価する処理がなされる。次にSA89へ進み、評価の結果その新たなCMの入手を希望するか否かの判断がなされ、希望しない場合にはSA83へ進むが、希望する場合にはSA90へ進み、希望するCMのユーザ宅17への送信方法として、電波メディア(無線系メディア)を利用するか否かの判断がなされる。利用しない場合には、SA93により、希望するCMをインターネット13経由でパソコン14へ送信する処理がなされた後SA83へ進む。一方、電波メディアを利用する場合にはSA91へ進み、常駐エージェント59とmeetingして、入手希望のCMの放送日時とチャンネルを教えもらい、SA92により、その放送日時とチャンネルと記録指示とをインターネット13経由でパソコン14へ送信する処理がなされた後SA83へ進む。

【0116】SA83により、新たなCM作成がないと判断された場合にはSA84へ進み、駐在を終了させるか否かの判断がなされ、ユーザエージェント26の駐在をまだ続行させる場合にはSA83へ進むが、駐在を終了させる場合にはSA85へ進み、駐在しているユーザエージェント26自身を消去する処理がなされて制御が終了する。

【0117】図11(a)はCMプレース58上の常駐エージェント59の動作を示すフローチャートであり、図11(b)は、CM制作者10の情報処理コンピュータ55の制御動作を示すフローチャートである。

【0118】まずCMプレース58に常駐している常駐エージェント59の動作を説明する。

【0119】SD1により、新たなCMが制作されたか否かの判断がなされ、制作されていない場合にはSD3に進むが、制作されている場合にはSD2に進む。SD2では、CMプレース58に駐在しているユーザエージェント26とmeetingして、新たなCMが制作された旨を知らせる処理がなされる。次にSD3に進み、CM放送日時とチャンネルの通知依頼があったか否かの判断がなされ、なかった場合にはSD1に戻る。一方、前述したSA79またはSA93に基づいてユーザエージェント26がCM放送日時とチャンネルの通知依頼を行なった場合には、SD3によりYESの判断がなされてSD4に進む。

【0120】SD4では、通知依頼のあったCMが既に放送が予定されているものであるか否かの判断がなされる。既に放送が予定されているもの場合には、放送予定日時とチャンネルが既に決まっているために、SD5に進み、その放送予定日時とチャンネルをCMプレース58にいるユーザエージェント26に通知する処理がなされた後SD1に戻る。

【0121】一方、放送が予定されていない場合にはSD6に進み、放送局2にCMを送信して放送依頼を行なう処理がなされる。次にSD7に進み、放送日時とチャンネルの返信があったか否かの判断がなされ、返信があるまで待機する。放送依頼を受けた放送局2は、その依頼されたCMをいつ放送するかの予定を立て、決まれば放送日時とチャンネルとをCM制作者10のCMプレース58の常駐エージェント59のにその旨を送信する。すると、SD7によりYESの判断がなされてSD8に進み、CM番号毎に分類して返信されてきた放送日時とチャンネルとを記憶する処理がなされる。次にSD9に進み、放送日時とチャンネルをCMプレース58上のユーザエージェント26に通知する処理がなされた後SD1に戻る。

【0122】次に情報処理コンピュータ55の動作を説明する。SE1により、番組関連データを受信したか否かの判断がなされ、受信していない場合にはSE4へ進む。図1で説明したように、番組関連データ制作者11からCM制作者10に番組関連データが送信されて来れば、SE1によりYESの判断がなされてSE2に進み、対応する番組のCMをデータベース56から検索してそのCMと受信したデータである番組関連データとを重合させる処理を行なう。その結果、データベース56内のCMは、番組関連データが重合されたCMデータとなる。また同じCMでも、どの番組に対し放映されるCMかによって番組関連データが異なるため、同じCMでも、対象となる番組毎に異なった番組関連データが重合された複数のCMデータがデータベース56に格納されることとなる。その結果、前述したCD6に従って放送局に送信されるCMは、そのCMに対応する番組の番組関連データが重合されたCMデータとなる。また、ユーザエージェント26が常駐エージェント59に対しCM放送日時とチャンネルの通知依頼を行なう場合には、どの番組に挿入して放映するCMであるかを通知する。常駐エージェント59は、その対象となる番組に対応した番組関連データが重合されたCMデータをデータベース56から検索して放送局2へ送信する。なお、データベース56を2分割して、CMのみが格納されたCM専用データベースと番組関連データ制作者11から送信されてきた番組関連データのみを格納した番組関連データ専用データベースとで構成し、ユーザエージェント26からのCM放送日時とチャンネルの通知依頼を受けたときに、そのCMの挿入放映の対象となる番組に関する番組

関連データを常駐エージェント59が検索し、ユーザーエージェント26により検索されたCMデータと常駐エージェント59が検索した番組関連データとを重合させて放送局2へ送信するようにしてもよい。次にSE3に進み、重合したCMのうち番組とともに放送するCMを放送局2へ送信する処理がなされる。つまり、番組の合間に挿入されて放送されるCMがこのSE3により放送局に送信され、放送局2から番組の放送とともに番組関連データが重合されたCMが放送される。

【0123】次にSE4に進み、新たに制作されたCMのデータベース56への入力があったか否かの判断がなされ、ない場合にはSE1に戻る。一方、入力があった場合にはSE5に進み、その新たなCMをデータベース56に記録する処理がなされ、次にSE6に進み、その新たなCMが制作された旨を常駐エージェント59に通知する処理がなされた後SE1に戻る。

【0124】図12は、前述したSE2により番組関連データが重合されたCMを受信してユーザ宅17のパソコン14のCRT52またはTV16によりそのCMを放映した画面図である。この図12では、パソコン14のCRT52によりCMを放映した画面図が示されている。この図12の場合には、コロンボ警部という主人公が登場するサスペンス番組の合間に挿入されるスーツのCMの場合である。そして、パソコン14のユーザが、来年大学を卒業して社会人一年生となる者であり、来年卒業する情報がユーザのプロフィール情報としてユーザエージェント26が知識として保有している。

【0125】ゆえに、ユーザエージェント26は、その来年卒業という知識に基づいて図12に示すようなCMを検索した。そして、番組関連データとして、この番組の意見交換用のホームページのアドレスを表示せたり(図12(a)参照)、このCMの放映の次に放映される番組部分で内容上注目すべき箇所、たとえば「殺人現場でのコロンボ警部の右手に注目下さい」のメッセージ表示を行なったりする(図12(b)参照)。また、図12(c)に示すように、番組に出てくる専門用語の説明、たとえば「サブリミナル効果: 人間が意識できない一瞬だけ映像を挿入して潜在意識に訴える」の文字表示等を行なってもよい。このように、SE2による重合とは、図12に示すように、CMの映像と文字情報等の重合である。

【0126】図13は、図2に示したコンテンツ提供者7の通信装置3とユーザのパソコン14との制御回路を示すブロック図である。通信装置3は、可変長データ生成部31、乱数取得部32、暗号処理部33、論理回路34、通信制御部35、認証処理部36、およびマスターキー暗号処理部37を備えている。

【0127】可変長データ生成部31は、移動先エージェント27による選択コンテンツの送信指令(SA38参照)に基づいてテレスクリプト・エンジン18から伝

送されてくるコンテンツの通信容量に応じたサイズの可変長データを生成する。たとえば静止画像の場合は画像1枚毎、動画画像の場合は1表示画面毎に可変長データを生成する。この可変長データは任意のビット列からなるデジタルデータである。乱数取得部32は、コンテンツを発振する度に乱数発生装置4から自然乱数を取得する。暗号処理部33は、可変長データおよび自然乱数に基づいて可変長乱数列を生成する。暗号化に際してはSXAL/MBAL(後述する)を使用する。

【0128】論理回路34は、テレスクリプト・エンジン18から伝送されてきたコンテンツの個々のビットと暗号処理部33により生成された可変長乱数列との排他的論理和(イクスクルーシブオア)を判定することで当該コンテンツをストリーム暗号化するものである。このストリーム暗号化された情報を伝送情報とする。通信制御部35は、各ユーザのパソコン14に対して通信設定して前記伝送情報や後述の通知情報を送信するとともに、各ユーザのパソコン14から送られる情報を受信するものである。

【0129】認証処理部36は、ユーザのアクセス制御等に際してのユーザ認証を行なうための処理部である。マスターキー暗号処理部37は、認証処理部36および会員管理センター12の管理サーバー69による認証の結果が正統の場合に暗号処理部33において使用された可変長データと自然乱数(複数の場合にはその使用順の情報を含む)を伝送マスターキーとし、これを当該ユーザに固有の鍵に基づいて暗号化するとともに、その暗号化により得られた情報を通知情報として通信制御部35から当該ユーザのパソコン14に対して送信するものである。暗号化にはSXAL/MBAL(後述する)を用いる。

【0130】会員管理センター12には、会員となっているユーザのIDやユーザ認証のための種々の会員情報がユーザ毎に分類して格納されているデータベース70が設置されている。管理サーバー69は、このデータベース70にアクセスして格納情報を検索してユーザ認証を行ない、その結果をインターネット13を経由して通信制御部30を介して認証処理部36へ送信する。

【0131】ユーザのパソコン14には、制御中枢としてのCPU60、プログラムが格納されているROM61、CPU60のワーキングエリアとしてのRAM62、ならびに電氣的に記憶データの消去が可能なEEPROM63が設けられている。さらに、外部との信号の整合性をとるための入出力インターフェイス64が設けられている。なお、クロック発生回路、アドレスデコード回路、パワーオンリセット回路等は図示を省略している。

【0132】入出力インターフェイス64には、カードリーダーライタ66が接続されており、ユーザのICカード65との信号のやり取りがこのカードリーダーライタ6

31

6, 入出力インターフェイス64を介してCPU60との間で行なわれる。入出力インターフェイス64にはフロッピーディスクリダライタ67が接続されており、フロッピーディスクに対する情報の読取および書込が可能となる。

【0133】入出力インターフェイス64にはハードディスクリダライタ68が接続されており、ハードディスクに対する情報の読取および書込が可能となる。入出力インターフェイス64にはキーボード53が接続されており、ユーザがキーボード53を操作することにより、その操作信号が入出力インターフェイス64を介してCPU60へ入力される。入出力インターフェイス64にはCRT52が接続されており、CRT表示用制御信号がCPU60から入出力インターフェイス64を介してこのCRT52へ与えられる。入出力インターフェイス64にはCD-ROMリダ68aが接続されており、CD-ROM68bの記録情報が読取可能となる。このCD-ROM68bには、前述したユーザエージェント26が記録されている。ユーザエージェント26は、このCD-ROM68bに記録された状態でエージェント製造業者からユーザに販売される。なお、ユーザエージェント26の販売は、CD-ROM68bに記録させた形で販売に代えて、エージェント製造業者がインターネット13を経由してオンラインによりユーザエージェント26を配信して販売してもよい。

【0134】図14は、ユーザが所有するICカード65の制御回路および記憶データを示す図である。ICカード65には、制御中枢としてのCPU91と、制御用のプログラムを記憶しているROM92と、CPU91のワーキングエリアとしてのRAM93と、電気的に記憶データの消去が可能なEEPROM94と、外部との信号の入出力を行なうためのI/Oポート90とが設けられている。ROM92には、ICカード65のためのOS(オペレーティングシステム)が記憶されている。このOSは、事実上の世界標準であるたとえばMULTOS(マルチ・アプリケーションICカードの汎用オペレーティング・システム)等のICカード汎用OSを用いるのが望ましい。

【0135】そして、たとえばEEPROM94には、必要に応じて各種のアプリケーションソフト95が記憶される。アプリケーションソフトとしては、たとえば、クレジット、デビット(預金自動引き落とし)、モンデックス、アクセス制御等の各種ソフトや、電子認証書、エージェント用知識データ、電子カルテ等の各種データが考えられる。これら各種アプリケーションソフトは、必要に応じて他の種類のアプリケーションソフトに書換えられるように構成されている。

【0136】エージェント用知識データ96としては、秘密性を要しない公表可能情報NSIと、秘密性を要する秘密情報SIとに分類されて記憶されている。公表可

32

能情報NSIとしては、たとえば、ユーザの職業、趣味、住所、音楽の好み、映画の好み、…ユーザの公開鍵PKU等である。秘密情報SIとしては、たとえば、ユーザの年収、電話番号、異性の好み、学歴、貯蓄額、財産、…ユーザの秘密鍵SKU等が考えられる。この秘密情報SIは、ユーザ固有の秘密鍵であるSK1により暗号化された状態で記憶されている。

【0137】ユーザは、自己のユーザエージェント26を利用する場合には、たとえばCD-ROM68bに記録されているユーザエージェントをCD-ROMリダ68aで読取らせ、さらに自己が所有しているICカード65をパソコン14のICカード挿入口50に挿入して、エージェント用知識データ96を読取らせ、ユーザエージェント96にエージェント用知識データ96を保有させた状態で、ユーザエージェント26を動作させる。このユーザのプロフィール情報96は、転職や引越等があればユーザが職業や住所等を書換えて更新する操作を行なう。また、ユーザエージェント26は、ユーザのために仕事をしないその結果をユーザに提供するのであり、その提供された結果に対するユーザの反応(満足するかまたは不満に思うか等)を観察し、必要があればユーザエージェント26自身がユーザのプロフィール情報96を更新したり補充したりする。その結果、ユーザエージェント26をユーザが活用すればするほどユーザのプロフィール情報96がユーザに適した内容のものとなり、ユーザエージェント26を活用すればするほどユーザの満足のいく仕事を行なうものとなる。

【0138】さらに、ユーザエージェント26が、仕事の結果を提供したユーザの反応(満足するかまたは不満に思うか等)を観察し、ユーザのプロフィール情報96ばかりでなく、ユーザエージェント26自身のプログラムを改良するといういわゆる機械学習を応用したものである場合には、ユーザエージェント26を、EEPROM63等の情報の書換えが可能な記憶媒体に記憶させておく必要がある。

【0139】また、図14に示したユーザのプロフィール情報96は、どのアドレスにどの種類のプロフィール情報が記憶されているかあるいはどのようなデータ構造で記憶させるか等が、世界的規模で統一化されたフォーマットに従っている。

【0140】図15は、前述したSXAL/MBALの概要を示す説明図である。図示の例では、平文データである20バイトの可変長データを8バイト(64ビット)の暗号鍵Kを用いて暗号化して20バイトの可変長暗号列を求める。図中、P、E、F、G、H、I、Cは各変換過程におけるデータであり、その添字はバイト数を表わしている。また、f mは暗号関数である。

【0141】図15を参照して、まず、可変長データPの左端の8バイトと拡大鍵KOとの排他的論理和(イクスクルーシブオア)を判定し、判定結果を関数f mによ

りデータ変換する。次に両端の各4バイトを合せてSXALによりデータ変換し、残りはそのままとする。続いてデータの順番を逆にし、暗号関数 f_m によりデータ変換した後、データの順番を逆にする。これを暗号関数 f_m によりデータ変換し、変換後のデータの左端の8バイトと拡大鍵 KI との排他的論理和(イクスクルーシブオア)を判定し、暗号化された可変長暗号列 C を求める。

【0142】本実施の形態では、前記暗号アルゴリズムが、16バイト以上のデータまたはファイルを1単位として暗号化するためメガバイト級の大容量毎の暗号化が可能で、前述のように双方向のデータ入換えを複数回実施して暗号化してから解読が著しく困難となる点、および情報伝達形態において1ビット程度のビット化けやデータ改ざんに遭遇した場合にすべての情報の正常復号が不可能となる点に着目して、これを大容量情報の高速伝達を行なう場合のセキュリティ確保に用いるようにしたものである。特に、1ビット程度のビット化けやデータ改ざんに遭遇した場合、DES型の暗号アルゴリズムでは、復号の際にビット化けや改ざん部分の近辺またはその部分以外のみが正常に復号されないため、受信側での異常感知が著しく困難となる。これに対し、SXAL/MBALでは、すべての部分が異常情報に変わるためその感知が極めて容易であり、通信中の場合は再送要求、ファイルの場合は保管中のバックアップファイルを使用するなど、迅速な対応が可能となる。

【0143】図16は、図13に示した送信装置3の動作を示すフローチャートである。SF1により、コンテンツの送信指令があったか否かの判断がなされ、ない場合にはSF14に進み、ユーザ認証処理を行なった後SF1へ戻る。このSF1、SF14のループの巡回途中で、前述したようにテレスクリプト・エンジン18からコンテンツの送信指令があった場合には、SF2に進み、その指令されたコンテンツが既に放送予定となっているコンテンツであるか否かの判断がなされる。既に放送予定となっているコンテンツの場合には、放送日時とチャンネルが放送局2からコンテンツ提供者7へ送信されてきているために、その放送日時とチャンネルをユーザのパソコン14へ送信した後SF1へ戻る。

【0144】一方、送信指令を受けたコンテンツが未だに放送予定となっていない新たなコンテンツである場合にはSF4へ進み、その選択されたコンテンツの送信単位、たとえば1フレーム F_s に対応する可変長データ(11111111)を生成する。次にSF5へ進み、乱数発生装置4からたとえば2つの自然乱数(R_1, R_2)を取得して、暗号処理を行なう。具体的には、可変長データを最初の自然乱数 R_1 を鍵(暗号鍵)として前述したSXAL/MBALにより暗号化し、初期乱数列 k_d0 (図15の下段の可変長暗号列 C に相当)を生成する。次に、SF7へ進み、初期乱数列 k_d0 の該当バイトと基準論理値 $01h$ との排他的論理和(イクス

クルーシブオア)判定により乱数列 $KS (=k_d1, k_d2, \dots, k_{di})$ を生成する。

【0145】ここで k_d1 は k_d0 の1バイト目と $01h$ との排他的論理和(イクスクルーシブオア)の判定結果、 k_d2 は k_d0 の2バイト目と $01h$ との排他的論理和判定結果、…である。さらに乱数列 KS を次の自然乱数 R_2 を鍵(暗号鍵)としてSXAL/MBALにより暗号化し、新たな乱数列 $RS (=r_d1, r_d2, \dots, r_{dn})$ を生成する(SF8)。ここで r_d1 は k_d1 の暗号処理結果、 r_d2 は k_d2 の暗号処理結果、 r_{dn} はデータ量調整されたデータ k_{di} の暗号結果、…である。

【0146】次にSF9へ進み、前述のようにして生成された乱数列 RS と送信単位 F_s との排他的論理和条件を判定して伝送情報 R_{Dn} を生成し、SF10へ進み、生成された伝送情報 R_{Dn} を放送局2へ送信する。放送局2では、伝送情報 R_{Dn} を受信して、それをいつどのチャンネルで放送するかを決定し、その決定された放送日時とチャンネルをコンテンツ提供者7へ返信してくる。その返信があればSF11によりYESの判断がなされてSF12へ進み、コンテンツNO。毎に分類して放送日時、チャンネルを記憶する処理がなされる。次にSF13に進み、その放送日時とチャンネルをユーザのパソコン14へ送信する処理がなされた後SF1へ戻る。

【0147】図17は、ユーザのパソコン14によるコンテンツ再生処理動作を示すフローチャートであり、図3に示したS20の具体的なフローチャートである。S25により、可変長データと乱数(R_1, R_2)の記憶があるか否かの判断がなされる。この両データは、ユーザのパソコン14を使用してユーザ認証が行なわれた結果適正である旨の判定がなされたことを条件として後述するようにコンテンツ提供者7からユーザのパソコン14へ送られてくるものである。この両データの記憶がない場合にはS26へ進み、まずユーザ認証処理(図18に基づいて後述する)を行なった後、S27へ進む。

【0148】S27では、可変長データを最初の自然乱数 R_1 によりSXAL/MBALにより暗号化し、初期乱数列 k_d0 を生成する。次に、S28へ進み、初期乱数列 k_d0 の該当バイトと基準論理値 $01h$ との排他的論理和(イクスクルーシブオア)判定により乱数列 $KS (=k_d1, k_d2, \dots, k_{di})$ を生成する。次にS29へ進み、乱数列 KS を次の自然乱数 R_2 を鍵としてSXAL/MBALにより暗号化し、新たな乱数列 $RS (=r_d1, r_d2, \dots, r_{dn})$ を生成する。前記初期乱数列 k_d0 、乱数列 k_s, r_s は、それぞれ図16に基づいて説明したものと同一のものである。

【0149】このようにして生成された乱数列 RS と受信した伝送情報 R_{Dn} との排他的論理和条件を判定して送信単位 F_s を生成し(S30)、コンテンツを再生す

10

20

30

40

50

る(S31)。

【0150】図18は、ユーザ認証処理を示すフローチャートであり、前述したSF14、S26の具体的な動作を示すフローチャートである。このフローチャートは、ユーザのパソコン14とコンテンツ提供者7の通信装置3と会員管理センター12の管理サーバー69それぞれのフローチャートである。

【0151】ユーザは、まず自己のICカード65をパソコン14のICカード挿入口50へ挿入する。その状態で、ユーザが暗証番号等を入力してカード認証を行ない、そのカード認証の結果適正である旨の判定がなされたことを条件としてS32の処理がなされる。S32では、ICカード65に記憶されている会員IDを読み出し、その読み出した会員IDと選択されたコンテンツNO.とをコンテンツ提供者7の通信装置3へ送信する処理がなされる。通信装置3では、SF15により、送信されてきたそれら情報を会員管理センター12の管理サーバー69へ中継して送信する処理が行なわれる。管理サーバー69では、SH1により、データベース70に格納されている会員管理用の情報を参照して送られてきた会員IDを確認し、適正である旨の確認が行なわれたことを条件として乱数を生成してチャレンジコードCCとして送信する処理がなされる。

【0152】コンテンツ提供者7の通信装置3では、SF16により、そのチャレンジコードCCを中継してユーザのパソコン14へ送信する。ユーザのパソコン14では、S33により、ICカード65内に記憶されているユーザのネットキーSKを呼出し、それを鍵を使用してレスポンスコードRCを生成して返信する処理がなされる。この処理は、 $RC = E_{SK}(CC)$ を演算し、その演算結果を返信する処理である。

【0153】コンテンツ提供者7の通信装置3では、そのレスポンスコードRCをSF17により中継して会員管理センター12の管理サーバー69に伝送する処理がなされる。

【0154】管理サーバー69では、SH2により、その送信されてきたレスポンスコードRCに基づいてユーザの本人認証を行なって確認し、適正である旨の確認ができればその旨をコンテンツ提供者7の通信装置3へ返信する処理がなされる。このSH2の処理は、具体的には、 $RC = D_{SK}(CC)$ が成立するか否かに基づいて行なう。なお、ネットキーSKは、会員管理センター12のデータベース70に会員のID毎に分類して格納されており、管理サーバー69が会員IDに相当するSKを検索してそれを用いてユーザ認証を行なう。

【0155】ユーザ認証の確認情報を受取ったコンテンツ提供者7の通信装置3では、SF18により、ユーザが希望するコンテンツに対応する可変長データKHと乱数(R1, R2)をユーザのネットキーSKで暗号化して秘匿した形態でユーザのパソコン14へ転送する処

理がなされる。ユーザのパソコン14では、S34により、その転送されてきた情報をネットキーSKにより復号化し、可変長データK1と乱数(R1, R2)とを再生して記憶する処理がなされる。このK1と乱数(R1, R2)とが前述した図17に示したS27以降の処理に利用される。

【0156】図19は、たとえば有料コンテンツを購入したユーザが、他のユーザにそのコンテンツを複製して配布するという不正コピーを防止するための制御回路である。この制御回路は、たとえばユーザのパソコン14に内蔵されている。コンテンツ提供者7が提供する有料コンテンツあるいは放送局2が放送する有料番組をユーザのパソコン14が受信してそのコンテンツをハードディスク81等に記録させる。前述したように、有料コンテンツの場合には、一般的に暗号化されたデータとして転送されてくるために、その転送データをそのまま暗号化された状態でパソコン14がハードディスク81に記録する。このハードディスク81から読み出された情報は、図17で説明したように、所定の復号化手段81aにより復号化され、コンテンツが再生される。

【0157】この復号化された後のコンテンツには、いわゆる電子透かし技術により、制御信号CCS(Copy Control Signal)を透かし情報として埋込んでいる。一般的に、透かし情報は、MEPG2による復号化を行なうことにより読み出すことができる。この復号手段81aにより復号化されたコンテンツデータがMEPG2復号化器82に入力され、復号化された情報を電子透かし検出器83に入力することにより、透かし情報である制御信号CCSを検出することができる。そしてその電子透かし検出器83により検出されたCCSがAPS86に入力される。このAPSは、たとえば米Macrovision Corp.が開発したAnalog Protection Systemであり、複製防止処理を行なうものである。

【0158】電子透かし検出器83からグラフィックス・モジュール84に、透かし情報を含むコンテンツデータが与えられ、グラフィックス・モジュール84からコンテンツデータがNTSC(National Television System Committee)符号化器85に与えられ、NTSC信号に変換される。そしてNTSC信号がパソコン14のCRT52、TV16、VTR15等へ供給される。

【0159】APS86に与えられるCCSは、たとえば、「コピー禁止」や「1度だけコピー可能」などのコピー制御信号であり、この信号に従ってAPS86が動作してCCSのデータ内容どおりのコピー禁止等の制御を行なう。

【0160】図20は、コンテンツ提供者7と第三者機関8あるいは放送局2と番組関連データ制作者11との間での情報のやり取りを無線系メディアを用いて行なう例を示す説明図である。この図20は、いわゆるワイヤレス・ローカル網WLL(Wireless Local Loop)を

利用したものを示している。コンテンツ提供者7、第三者機関8、放送局2、番組関連データ制作者1.1には、それぞれ、無線装置71、72、74、75が設けられている。そして、前述したように、第三者機関8とコンテンツ提供者7との間での、ユーザエージェント26、有料コンテンツ、第三者機関エージェント29等の伝送を、このWLLを利用して行なう。図中76、77、78、79、80はWLL用のアンテナである。

【0161】また、放送局2と番組関連データ制作者1.1との間での、番組関連データの伝送等も、WLLを利用して行なう。なお、1は衛星、5は衛星用のアンテナである。

【0162】第三者機関8とコンテンツ提供者7との間での情報のやり取りは、多数のユーザエージェントや多数の第三者機関エージェントや多数のコンテンツが比較的大量に集まって送受信されるために、そのような大量のデータをこのWLLを利用して送受信することにより、効率的に送受信できる利点がある。

【0163】図21は、不正コピー防止のための他の例を示す制御回路図である。この制御回路も、たとえばユーザのパソコン14に内蔵されている。ユーザのパソコン14で受信した暗号化されたコンテンツデータは前述したようにハードディスク81に記録される。この暗号化コンテンツデータ内には、その暗号化コンテンツを復号化するための前述した可変長データK1、乱数R1、R2が前述したユーザのネットキーSKで暗号化された状態で、透かし情報として組込まれている。

【0164】ハードディスク81に記録されているこのような暗号化コンテンツデータがMP EG2復号化器82に入力され、そこで復号化されて透かし情報が検出可能な状態に変換され、そのデータが電子透かし検出器83に入力され、透かし情報であるE_{sk}(K1、R1、R2)が検出されてパソコン14のCRT52、TV16に入力される。一方、電子透かし検出器83からの暗号化コンテンツデータがグラフィックス・モジュール84を経由してNTSC符号化器85に入力され、NTSC信号としてCRT52、TV16、VTR15に与えられる。このNTSC信号は、暗号化されたコンテンツデータのNTSC信号であるために、このNTSC信号に基づいてそのままCRT52、TV16等により放映したとしても、暗号化されたデータに従った映像しか放映されず、ユーザが何ら認識できない映像となる。

【0165】そこで、たとえばユーザのパソコン14のICカード挿入口50にユーザのICカード65を挿入することにより、そのICカード65に記憶されているユーザのネットキーSKがパソコン14により読取られ、パソコン14に入力されたE_{sk}(K1、R1、R2)をユーザのネットキーSKより符号化してK1、R1、R2を再生し、それらデータを用いてNTSC信号を復号化して通常のコンテンツデータに対するNTSC

信号に変換し、それに基づいてCRT52により映像を表示するように制御する。

【0166】TV16にもICカード挿入口を形成し、そこにICカード65を挿入することにより、前述と同様にTV16によりNTSC信号を復号化して通常のコンテンツデータに対するNTSC信号に変換して放映する。

【0167】このように構成することにより、有料コンテンツを正規に購入したユーザのICカード65を、パソコン14あるいはTV16に挿入しない限り、有料コンテンツを再生して放映することができない。なお、VTR15には、ICカード挿入口が形成されていないため、VTR15に記録されるデータは暗号化されたコンテンツに対するNTSC信号となる。そしてこのVTR15に記録されている暗号化されたコンテンツに対するNTSC信号をCRT52あるいはTV16により再生する際には、ICカード60を挿入して前述したように復号化して再生閲覧する。

【0168】この図21に示す別実施の形態により、TV16でコンテンツを再生する場合には、TV16に図17に示したコンテンツ再生処理の機能が内蔵されることとなる。また、CRT52によりコンテンツを再生する場合には、パソコン14のICカード挿入口50にICカード65を挿入して再生するのであるが、図21に示すように、NTSC符号化器85からCRT52に供給されたNTSC信号に対し復号化を行なうようにし、パソコン14内でNTSC信号が復号化されてその復号化されたNTSC信号がたとえばTV16やVTR15に出力できないように構成されている。

【0169】また、この図21に示す別実施の形態では、図18に示したユーザ認証処理を行なって適正なユーザである旨の認証が行なわれた後、可変長データK1と乱数(R1、R2)とをユーザのネットキーSKで暗号化したデータを暗号化コンテンツデータに透かし情報として組込んでその情報を放送局2等を経由してユーザのパソコン14に転送するようにする。

【0170】図22～図24は、図16～図18に示した制御動作の他の例を示す図である。

【0171】図22は、コンテンツ提供者7の通信装置3の動作を示すフローチャートであり、図16と対応している。SF19により、コンテンツの送信指令があったか否かの判断がなされ、ない場合にはSF19aに進み、ユーザ認証処理を行なった後SF19へ戻る。

【0172】テレスクリプト・エンジン81からコンテンツの送信指令があった場合にはSF20へ進み、既に放送予定となっているコンテンツであるか否かの判断がなされ、放送予定となっているコンテンツである場合にはSF21へ進み、放送日時とチャンネルをパソコン14へ送信してSF19へ戻る。一方、未だに放送予定となっていない新しいコンテンツについて送信指令があつ

た場合にはSF22へ進み、ユーザの秘密鍵SKUと同じビット数の乱数RNを生成する処理がなされる。一般的にRSA等の公開鍵暗号方式で用いられる秘密鍵のビット数は、1024ビットであるために、このSF22で生成される乱数RNも1024ビットになる可能性が高い。

【0173】次にSF23へ進み、選択されたコンテンツをユーザの秘密鍵SKUと同じビット数(たとえば1024ビット)ずつに分割して分割コンテンツA(=A1, A2, ...An)を生成する処理がなされる。SKUと同じビット数に分割した場合には、コンテンツに端数が生ずるのが一般的である。その場合には、最後の分割コンテンツAnがSKUのビット数よりも少ないビット数のデータとなる。次にSF24へ進み、分割コンテンツAとSF22により生成された乱数RNとの排他的論理和(イクスクルーシブオア)を演算する。図22～図24ではイクスクルーシブオアとして○の中に+が描かれた記号を用いているが、明細書では(+)の記号を用いる。SF24の具体的演算内容は、分割コンテンツA1, A2, ...Anのそれぞれと乱数RNとのイクスクルーシブオアを計算するものである。次にSF25へ進み、SF24による演算結果A(+)RNを放送局2へ送信する処理がなされる。これを受けた放送局2は、A(+)RNを放送する日時とチャンネルを決定し、その決定された放送日時とチャンネルをコンテンツ提供者7に返信する。その返信があれば、SF26によりYESの判断がなされてSF27へ進み、コンテンツNO、毎に分類して放送日時とチャンネルを記憶する処理がなされ、SF28に進み、その放送日時とチャンネルをパソコン14へ送信する処理がなされた後SF19へ戻る。

【0174】なお、SF24の最後のAn(+)RNは、分割コンテンツデータAnが端数の関係上SKUよりも少ないビット数の分割コンテンツである場合には、乱数RNの先頭から分割コンテンツAnのビット数だけのデータを取り出し、そのデータとAnのイクスクルーシブオアを演算する。

【0175】図23は、SF19aおよび後述するS36に示されたユーザ認証処理の具体的動作を示すフローチャートであり、図18と対応している。

【0176】まずユーザが自己のICカード65をパソコン14のICカード挿入口50に挿入して前述と同様にカード認証を行ない、適正である旨の認証が行なわれたことを条件としてS38により、挿入されたICカード65に記憶されているユーザのIDが読取られてその会員IDと選択されたコンテンツNO、とがコンテンツ提供者7の通信装置3へ送信される。通信装置3では、その送信されてきた情報をSF19により中継して会員管理センター12の管理サーバー69に伝送する。管理サーバー69では、SH3により、データベース7

0にアクセスして送られてきた会員IDを確認して適正であるか否かの判断を行ない、適正である旨の確認をした後乱数を生成してチャレンジコードCCを通信装置3へ送信する。

【0177】通信装置3では、その送信されてきたチャレンジコードCCをSF20により中継してユーザのパソコン14へ送信する。ユーザのパソコン14では、S39により、ICカード内のネットキーSKを読み出し、そのSKを鍵としてレスポンスコードRCを生成して返信する処理がなされる。つまり、 $RC = E_{SK}(CC)$ を演算して返信する。通信装置3では、その返信されてきたRCをSF21により中継して管理サーバー69に送信する処理が行なわれる。管理サーバー69では、SH4により、その送信されてきたレスポンスコードRCに基づいてユーザの本人認証を行ない適正である旨の認証が行なわれたことを確認した場合にその旨を返信する処理がなされる。つまり、SH4では、 $CC = D_{SK}(RC)$ が成立するか否かを判断してユーザの本人認証が行なわれる。

【0178】通信装置3では、ユーザの本人認証の確認情報を受取れば、選択されたコンテンツをSF23同様に分割し、分割コンテンツA(=A1, A2, ...An)を管理サーバー69へ送信する処理がなされる。管理サーバー69では、SH5により、 $SKU(+) \{ I1(+) (A1(+) RN) \} = A1$
 $SKU(+) \{ I2(+) (A2(+) RN) \} = A2$

$SKU(+) \{ In(+) (An(+) RN) \} = An$ を満たすI(=I1, I2, ...In)を演算して、 $E_{SK}(I)$ を通信装置3へ送信する処理がなされる。

【0179】ここで、I1, I2, ...Inは、それぞれ、A1, A2, ...Anの分割コンテンツのビット数と同じビット数(たとえば1024ビット)のデータである。なお、端数の関係上Anが通常より少ないビット数であった場合には、InもAnに合せた少ないビット数となる。このI1, I2, ...Inの算出は、比較的簡単に行なえ得る。たとえば、SKUとA1とRNとの最上位ビットがともに「1」であった場合には、 $1(+) \{ I1 \text{の最上位ビット}(+) (1(+) 1) \}$

$= 1$

となり、I1の最上位ビットは自ずと「0」となる。また、SKUの最上位ビットの次のビットが0で、A1とRNとの最上位ビットの次のビットがともに1であった場合には、 $0(+) \{ I1 \text{の最上位ビットの次のビット}(+) (1(+) 1) \} = 1$

となり、I1の最上位ビットの次のビットは自ずと「1」となる。

【0180】通信装置3では、 $E_{SK}(I)$ を受けてSF23により中継してユーザのパソコン14へ送信する処

理がなされる。ユーザのパソコン14では、S40により、受信した情報を鍵SKにより復号化する処理、すなわち、 $T_{SK}\{E_{SK}(I)\}$ を演算してIを再生して記憶する処理がなされる。なお、この別実施の形態では、会員管理センター12のデータベース70に、会員のIDごとに分類して会員(ユーザ)の秘密鍵SKUが格納されている。この秘密鍵SKUは、秘密性が保持可能な状態でデータベース70に格納されており、会員管理センター12のある限られたオペレータのみが管理サーバー69によりSKUにアクセスできるように構成されている。 10

【0181】図24は、ユーザのパソコン14の動作を示すフローチャートであり、図17に示したフローチャートに対応したものである。まずS35により、 $I(=I_1, I_2, \dots, I_n)$ を記憶しているか否かの判断がなされる。図23に示したユーザ認証が終了した段階ではIがユーザのパソコン14により記憶されているために(S40参照)、S35によりYESの判断がなされてS37に進むが、まだIが記憶されていない場合にはS36に進み、図23に示したユーザ認証処理が行なわれ 20

た後S37へ進む。S37では、
 $A = SKU(+)\{I_1(+)(A_1(+))RN\}$
 $+SKU(+)\{I_2(+)(A_2(+))RN\}$
 $+SKU(+)\{I_3(+)(A_3(+))RN\}$
 \vdots
 $+SKU(+)\{I_N(+)(A_N(+))RN\}$
 を演算して、コンテンツを再生する処理がなされる。

【0182】この別実施の形態では、S37で示したように、コンテンツAを再生するには、当該ユーザの秘密鍵であるSKUが必要となる。つまりこのユーザの秘密鍵SKUを用いて暗号化コンテンツを復号化する処理がコンテンツAを再生するのに必須の処理となっている。その結果、暗号化コンテンツを正規に購入したユーザ以外のユーザが暗号化コンテンツを復号化してコンテンツAを再生するためには、当該暗号化コンテンツを購入した正規のユーザの秘密鍵SKUを用いて暗号化コンテンツを復号化せざるを得ず、正規のユーザからICカード65を入手しなければコンテンツAを得ることはできない。ゆえに、セキュリティが向上する。

【0183】この図22～図24の別実施例を別の表現で簡単に説明すれば、以下のようなものとなる。 40

【0184】コンテンツ提供者7が作成したコンテンツをAとし、コンテンツ提供者7は、その有料コンテンツAを乱数等からなる鍵RNにより暗号化して $E_{RN}(A)$ を演算してそれを放送局2から放送してもらう。またコンテンツ提供者7は、 $D_{SKU}[D_i\{E_{RN}(A)\}] = A$ を満たす鍵Iを生成し、それを鍵SKで暗号化してインターネット13等を経由してユーザのパソコン14へ送信する。

【0185】ユーザは、放送局2から受信したE 50

$RN(A)$ をコンテンツ提供者7から受信して再生した鍵Iで復号化し、さらにそれを自分の秘密鍵SKUで復号化する。その結果、コンテンツAを得ることができる。

【0186】なお、このようなRNやIやSKU等の鍵を用いて暗号化、復号化するアルゴリズムを、RSA公開鍵暗号方式やいわゆる楕円曲線暗号のアルゴリズムを用いれば、 $D_i\{E_{RN}(A)\} = E_{PKU}(A)$ が成立する。ゆえに、この式を満たすIをコンテンツ提供者7が算出してそれをユーザのパソコン14に送信すれば事足りることとなり、Iを生成するのにユーザの公開鍵PKUで事足りユーザの秘密鍵SKUを必要としないこととなる。

【0187】次に、以上説明した実施の形態の変形例や特徴点等を以下に列挙する。

(1) 前述した実施の形態では、CM制作者10が制作したCMに対し番組関連データ制作者11が制作した番組関連データを重合させて放送し、番組の合間に挿入されているCMをユーザがカットして番組の部分のみを閲覧する不都合を防止するためのCMカット閲覧防止システムの発明が開示されている。

【0188】この発明は、ユーザに閲覧を希望させるためのコンテンツの合間に商業メッセージを挿入して宣伝を行なう宣伝システム(宣伝方法)を発明の属する技術分野とする。

【0189】従来から一般的に知られている宣伝システム(宣伝方法)は、テレビ番組等の合間に商業メッセージ(CM)を挿入して放送局から放送し、ユーザがその放送を受信してTV(テレビジョン)で放映してCMを閲覧することにより、CMのスポンサーの宣伝やスポンサーの商品の宣伝を行なうものがあった。

【0190】一方、近年、ユーザの家庭にはVTR(ビデオテープレコーダ)が普及しており、放送局が放送したCMを含む番組を一旦このVTR等に記録させ、後日それを再生してTVやパソコン等で閲覧するという記録再生閲覧が増えてきた。

【0191】その結果、番組の合間に挿入されているCMはユーザにしてみれば贅肉に相当する部分であるために、そのCM部分のみをカットして番組部分のみを再生して閲覧するというCMカット閲覧が増えることが予想される。

【0192】このようなCMカット閲覧が増えた場合には、民放番組のスポンサーがCMによる利益を見込めなくなり、スポンサーによって成り立っている民放が崩壊するおそれがある。

【0193】つまり、従来の宣伝システム(宣伝方法)においては、ユーザに閲覧を希望させるためのコンテンツの合間に挿入された商業メッセージのみをユーザがカットしてコンテンツのみを閲覧するために、商業メッセージの挿入による利益が見込めなくな

るという欠点があった。

【0194】この宣伝システムの発明は、かかる実情に鑑み考え出されたものであり、その目的は、ユーザによる前述したCMカット閲覧を極力防止することである。

【0195】この目的を達成するための手段として、この宣伝システムの発明は、ユーザに閲覧を希望させるためのコンテンツの合間にコマーシャルメッセージを挿入して宣伝を行なう宣伝システムであって、前記コマーシャルメッセージが挿入される対象となる前記コンテンツに関連するコンテンツ関連情報を制作する制作者によって制作されたコンテンツ関連情報を前記コマーシャルメッセージと同時に放映する同時放映手段を含むことを特徴とする。

【0196】このような手段を採用した結果、コマーシャルメッセージと同時にそのコマーシャルメッセージが挿入されたコンテンツに関連するコンテンツ関連情報が放映される。コンテンツに興味のあるユーザはそのコンテンツ関連情報をも閲覧を希望するために、コンテンツ関連情報を閲覧すれば同時にコマーシャルメッセージも閲覧する結果となる。ゆえに、コマーシャルメッセージをカットしてコンテンツのみを閲覧することが極力防止できる。

【0197】前記同時放映手段は、前記コマーシャルメッセージが挿入される対象となる前記コンテンツ(番組)に関連するコンテンツ関連情報(番組の意見交換用のホームページや番組の重要なポイントに注意を促すメッセージや番組内に登場する専門用語の解説等)を制作する制作者(番組関連データ制作者11)によって制作されたコンテンツ関連情報を前記コマーシャルメッセージと重合させる重合手段(SE1, SE2)と、該重合手段により前記コンテンツ関連情報が重合されたコマーシャルメッセージを前記コンテンツの合間に放映する放映手段(SE3, SD3~SD9, 放送局2, パソコン14あるいはTV16)とを含んでいる。

【0198】前記重合手段は、たとえばテレビ番組の放映中に地震等が発生した旨の臨時ニュースのメッセージを文字情報として表示させるという従来から周知の文字作成装置等の重合手段を用いればよい。なお、前記重合手段は、前述した本実施の形態では、CM制作者10の所に設けられたものを示したが、その代わりに、放送局2に設けてもよい。その場合には、番組関連データ制作者11が制作した番組関連データをインターネット13を経由して放送局2に送信し、放送局2において放送するコマーシャルメッセージにその番組関連データを重合させて放送する。

【0199】また、前述したコマーシャルメッセージカット閲覧を防止する目的を達成する発明として、次のような手段を有するものであってもよい。

【0200】ユーザに閲覧を希望させるためのコンテンツの合間にコマーシャルメッセージを挿入して宣伝を行

なう宣伝方法であって、前記コマーシャルメッセージが挿入される対象となる前記コンテンツに関連するコンテンツ関連情報を生成するコンテンツ関連情報生成ステップと、該コンテンツ関連情報生成ステップにより生成された前記コンテンツ関連情報と前記コマーシャルメッセージとを重合させる重合ステップと、該重合ステップにより前記コンテンツ関連情報が重合した前記コマーシャルメッセージを前記コンテンツの合間に放映する放映ステップとを含むことを特徴とする、宣伝方法。

10 【0201】前述した番組関連データ制作者11が図12に示すような番組関連データを制作する説明部分により、前記コンテンツ関連情報生成ステップが構成されている。前記SE2により、前記重合ステップが構成される。前記SE3, SD3~SD9, 放送局2, 前記S13~S16により、前記放映ステップが構成される。

【0202】(2) 前述した本実施の形態では、ユーザが好むと思われるコマーシャルメッセージを検索してそのユーザに放映閲覧させるという発明が開示されている。この発明は、コマーシャルメッセージによりユーザ20に対し宣伝を行なう宣伝システム(宣伝方法)を発明の属する技術分野とする。

【0203】この種の宣伝システム(宣伝方法)において、従来から一般的に知られてるものに、たとえば、民放の番組に対するスポンサーのためのコマーシャルメッセージをCM制作者が制作し、その制作されたコマーシャルメッセージが放送局に提供されて番組の合間に挿入された状態で放送される。ユーザは、放送番組の中から閲覧を希望する放送を受信してTVやパソコン等により閲覧をし、その閲覧途中で挿入されたコマーシャルメッセージが放映されることにより、ユーザに対しスポンサーの宣伝を行なっていた。

【0204】しかし、この種の従来の宣伝システム(宣伝方法)では、CM制作者が一方的にスポンサーのCMを作成してユーザが好むと好まざるとにかかわらず一方的に制作されたCMを放送局から放送していた。その結果、ユーザにしてみれば、全く興味のない商品のCMや自分にほとんど無関係なCMを閲覧する状態となる。たとえば、アルコールを受けつけないユーザに対しビールの宣伝をしたところでユーザにとって全く無駄であるばかりでなくスポンサー側にとっても全く効果のないCMとなってしまう。このように、従来の宣伝システム(宣伝方法)は、ユーザ側およびスポンサー側双方にとって無駄の多い利益の少ないものとなってしまうという欠点があった。

【0205】本発明は、かかる実情に鑑み考え出されたものであり、その目的は、宣伝者側およびユーザ側の双方における無駄を極力防止することである。

【0206】この目的を達成する手段として、この発明は、コマーシャルメッセージによりユーザに対し宣伝を行なう宣伝システムであって、ユーザを複数種類の属性

毎に分類し、その分類毎に当該分類に属するユーザのみをターゲットにして制作されたコマーシャルメッセージを格納するコマーシャルメッセージ格納手段と、ユーザのプロフィール情報を知識として保有し、当該ユーザのために働くユーザエージェントに前記コマーシャルメッセージ格納手段に格納されているコマーシャルメッセージを検索させる検索手段と、該検索手段により検索されたコマーシャルメッセージを前記ユーザエージェントの持主であるユーザに提供するコマーシャルメッセージ提供手段とを含むことを特徴とする。

【0207】このような手段を採用した結果、複数種類の属性に分類されたユーザ毎に当該分類に属するユーザのみをターゲットにしてコマーシャルメッセージが制作され、ユーザエージェントによりそのような複数のコマーシャルメッセージの中からユーザが好むと思われるコマーシャルメッセージが検索されて選択され、ユーザに提供される。その結果、ユーザに適したきめ細かなコマーシャルメッセージがユーザ毎に提供可能となり、ユーザにとって不必要なコマーシャルメッセージがユーザに提供されてしまうという無駄を極力防止することができる。

【0208】前記データベース56により、ユーザを複数種類の属性毎に分類し、その分類毎に当該分類に属するユーザのみをターゲットにして制作されたコマーシャルメッセージを格納するコマーシャルメッセージ格納手段が構成されている。前記テレスク립ト・エンジン57により、ユーザのプロフィール情報を知識として保有し、当該ユーザのために働くユーザエージェント26に前記コマーシャルメッセージ格納手段に格納されているコマーシャルメッセージを検索させる検索手段が構成されている。前記SA76～SA80、SA89～SA93、インターネット13、放送局2、S2、S11～S16により、前記検索手段により検索されたコマーシャルメッセージを前記ユーザエージェントの持主であるユーザに提供するコマーシャルメッセージ提供手段が構成されている。

【0209】前記ユーザを複数種類の属性に分類する具体例としては、たとえば、ユーザを、年齢別、性別、学識レベル別、職業別、ユーザの消費動向別、ユーザの各種好みの嗜好別等に分類することが考えられる。番組等のコンテンツの合間に挿入されるコマーシャルメッセージの放映時間としては、たとえば、20秒、40秒、60秒、80秒、100秒等のように、複数種類の放映時間を予め規格化しておき、前記コマーシャルメッセージ格納手段に格納される複数のコマーシャルメッセージも、1つのメッセージまたは複数のメッセージを組合せて放映することにより前記規格化された時間にちょうど収まるような長さに制作しておく。

【0210】一方、放送局2からコマーシャルメッセージを含む番組を放送する場合には、番組放送からコマー

シャル放送に切替える直前にコマーシャルメッセージの放映時間を特定するデータを放送する。ユーザ側においては、パソコン14等により、そのコマーシャルメッセージの放映時間を特定する情報を受信してその情報に基づいて特定されるコマーシャルメッセージ放映時間だけユーザエージェントが検索したコマーシャルメッセージに切換えて放映する。

【0211】一方、ユーザエージェントが予め選択して予約した番組以外の番組をユーザが見る場合もあり、その場合に対応する方法としては、当日放送される番組のスポンサーすべてについてコマーシャルメッセージを予めユーザエージェントが検索してユーザのパソコン14のハードディスク等に記憶しておくことが考えられる。

【0212】コマーシャルメッセージの記憶は、1つのスポンサーに対し複数種類検索して記憶しておき、その複数種類のコマーシャルメッセージを入れ代わり立ち代わり放映してユーザが飽きないようにすることが望ましい。

【0213】一方、ユーザが全く不要とするコマーシャルメッセージたとえばアルコールを全く受けつけないユーザに対しビールやウイスキー等のコマーシャルメッセージは、当然ユーザエージェントが検索しない。その結果、そのようなユーザに対しては、ユーザが見ている番組のスポンサーになっているにもかかわらずそのユーザには当該スポンサーのコマーシャルメッセージが全く放映されないという不公平な事態が生ずる。そこで、たとえば一定の地域内等において、スポンサー同士コマーシャルメッセージの放映回数が平等となるように調整する調整手段を設置するのが望ましい。

【0214】図1に示した衛星放送を利用してコマーシャルメッセージを放映する方法として、たとえば、コマーシャルメッセージばかりを次々と放映する衛星放送を1チャンネルまたは多数チャンネルにわたって開設し、ユーザエージェントが前記コマーシャルメッセージ格納手段にアクセスして検索選択したコマーシャルメッセージが衛星放送によって放送される日時とチャンネルを特定できるデータをユーザのパソコンに送信する。ユーザのパソコン14では、送信されてきた日時が来れば送信されたチャンネルにチューニングして放送電波をキャッチしてその放送内容であるコマーシャルメッセージをハードディスク等に記憶させる。

【0215】ほぼすべてのスポンサーについてコマーシャルメッセージをユーザエージェントが検索してユーザのパソコン14のハードディスク等に記憶した段階では、その後においては、あるスポンサーについて新たなコマーシャルメッセージが制作された場合に限り、その新たなコマーシャルメッセージについてユーザエージェントが検索し必要と判断すればこのコマーシャルメッセージをユーザのパソコン14のハードディスク等に記憶させる。またあるスポンサーについて古くなって消去さ

れたコマーシャルメッセージも、そのコマーシャルメッセージがパソコン14のハードディスクに記憶されておればそのハードディスクから消去する。

【0216】その場合、前記コマーシャルメッセージ格納手段において、新たに作成されて新たに格納されたコマーシャルメッセージあるいは古くて消去されたコマーシャルメッセージが生ずるごとに、たとえばプッシュ技術を利用してユーザのパソコン14にまでその旨を伝送する。ユーザのパソコン14では、その伝送されてきた情報に基づいてハードディスクの記憶内容を更新する。

【0217】さらに、ユーザエージェント26が検索したコマーシャルメッセージについてより詳細なデータを手に入れた場合には、インターフェイス13経由で所定のWWWサーバーへアクセスして入手できるようにするべく、そのコマーシャルメッセージについてのWWWサーバーのアドレスをユーザのパソコン14に伝送するのが望ましい。そのWWWサーバーのアドレスデータの送信は、たとえば衛星データ配信・放送を利用したり、テレビ放送用の地上波を利用したデータ多重放送により配信する。

【0218】(3) 前述した本実施の形態では、図22～図24に示したように、有料コンテンツ等の情報のセキュリティを確保するシステム(または方法)が開示されている。

【0219】この発明は、情報提供者側が情報要求者側に提供する情報に対するセキュリティシステム(またはセキュリティを確保する方法)を発明の属する技術分野とする。

【0220】この種のセキュリティを確保する技術として、従来から一般的に知られているものに、たとえば、あるユーザによって有料コンテンツが購入されれば、その有料コンテンツを暗号化してたとえば放送局からその暗号化コンテンツを放送してもらう。その暗号化コンテンツを購入したユーザに対しては、その暗号化コンテンツの放送日時とチャンネルとを事前に通知しておき、ユーザがその暗号化コンテンツの放送を受信して暗号化コンテンツをVTR等に記録する。そして、有料コンテンツの提供者が前記暗号化コンテンツを復号化して再生するための鍵を当該有料コンテンツを購入した正規のユーザに対し配信する。その正規のユーザは、その配信されてきた鍵を用いてVTR等に記録してある暗号化コンテンツを復号化して再生して閲覧する。

【0221】このような従来の技術の場合には、暗号化コンテンツが電波メディア(無線系メディア)により広域にわたって放送されるために、有料コンテンツに対する料金を支払った正規のユーザ以外のその他多数のユーザが暗号化された有料コンテンツを受信可能となる。このような正規のユーザ以外のその他多数のユーザが前述した暗号化された有料コンテンツを受信して記録した場合には、後はコンテンツ提供者から配信される暗号化

コンテンツを復号化するための鍵(以下単に復号化鍵という)をなんらかの方法で入手するだけで、暗号化コンテンツを復号化して再生閲覧することが可能となる。その結果、有料コンテンツに対し料金を支払っていない多数のユーザが有料コンテンツを再生閲覧可能となってしまうという不都合が生ずる。

【0222】そこで、前記復号化鍵FKを、料金を支払った正規のユーザの公開鍵PKUにより暗号化してE_{PKU}(FK)の形で前記正規のユーザにインターネット等を経由して配信することが考えられる。そのようにすれば、他の多数のユーザがこのE_{PKU}(FK)を傍受したとしても、料金を支払った正規のユーザの秘密鍵SKUをもっていない限り復号化して復号化鍵FKを再生することができず、一応セキュリティは保たれるように思われる。

【0223】しかし、あるグループの構成員全員が暗号化コンテンツデータの放送を受信し、その構成員の一人が代表として料金を支払ってE_{PKU}(FK)を受信し、その代表者の秘密鍵で復号化してD_{SKU}{E_{PKU}(FK)}を演算してFKを再生し、そのFKをグループの他の構成員全員に配信した場合には、一人分の料金しか払わないにもかかわらず大勢の人間が暗号化コンテンツデータを閲覧することが可能となる。

【0224】この発明は、かかる実情に鑑み考え出されたものであり、その目的は、有料コンテンツ等の情報を利用する権限を有する正規のもの以外のものが不正に情報利用することを極力防止することである。

【0225】このような目的を達成するべく、この発明は、次のような手段を採用している。

【0226】情報提供者側が情報要求者側に提供する情報に対するセキュリティを確保する方法であって、前記情報提供者側において第1の鍵を用いてあるアルゴリズムに従って前記情報を変換する変換ステップと、該変換ステップにより変換された変換情報を前記情報要求者側に提供する変換情報提供ステップと、前記情報提供者側において、第2の鍵を生成する第2の鍵生成ステップと、該第2の鍵生成ステップにより生成された前記第2の鍵を前記情報要求者側へ提供する第2の鍵提供ステップとを含み、前記第2の鍵生成ステップは、前記変換情報に対し、前記第2の鍵を用いてのあるアルゴリズムに従った変換処理と前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理とを施すことを条件として前記情報を再生できるように定められた前記第2の鍵を生成することを特徴とする、情報に対するセキュリティを確保する方法。

【0227】また、前述した目的を達成する他の手段として、本発明は以下の構成を採用してもよい。

【0228】情報提供者側が情報要求者側に提供する情報に対するセキュリティシステムであって、前記情報提供者側において第1の鍵を用いてあるアルゴリズムに

従って前記情報を変換する変換手段と、該変換手段により変換された変換情報を前記情報要求者側に提供する変換情報提供手段と、前記情報提供者側において、第2の鍵を生成する第2の鍵生成手段と、該第2の鍵生成手段により生成された前記第2の鍵を前記情報要求者側へ提供する第2の鍵提供手段とを含み、前記第2の鍵生成手段は、前記変換情報に対し、前記第2の鍵を用いてのあるアルゴリズムに従った変換処理と前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理とを施すことを条件として前記情報を再生できるように定められた前記第2の鍵を生成することを特徴とする、情報に対するセキュリティシステム。

【0229】本発明がこのような手段を採用した結果、暗号化情報を復号化して再生する際に、情報提供者側が前記情報を提供する相手である正規の情報要求者側の秘密鍵を用いての変換処理が必須となる。その結果、暗号化情報を復号化して再生するには、前記正規の情報要求者側の秘密鍵を入手しなければならない。しかし、秘密鍵というものは秘密性を保持しなければならない性質のものであり、他人にみだりに貸し与えて使用させることがあまり考えられないものである。ゆえに、前記正規の情報要求者以外の他の者が正規の情報要求者から秘密鍵を入手することは一般的にあまり考えられず、正規の情報要求者以外のものが前記暗号化情報を復号化して再生することが極力防止できる。

【0230】前記第2の鍵生成ステップ(第2の鍵生成手段)は、前記変換情報に対し、前記第2の鍵を用いてのあるアルゴリズムに従った変換処理が実行された後前記情報要求者側の秘密鍵を用いてのあるアルゴリズムに従った変換処理を施すことを条件として前記情報を再生できるように定められた前記第2の鍵を生成するものであることが望ましい。

【0231】前記SF22～SF24により、前記情報提供者(コンテンツ提供者7)側において第1の鍵(乱数RN)を用いてあるアルゴリズム(イクスクリューシブオア)に従って前記情報を変換する変換ステップ(変換手段)が構成されている。前記SF25～SF28、放送局2、S7、S23、S8、S24、S2、S11～S16により、前記変換ステップ(変換手段)より変換された変換情報(A(+)RN)を前記情報要求者(ユーザ)側に提供する変換情報提供ステップ(変換情報提供手段)が構成されている。

【0232】前記SH5により、前記情報提供者側において、第2の鍵を生成する第2の鍵生成ステップ(第2の鍵生成手段)が構成されている。SH5、SF23により、前記第2の鍵生成ステップ(第2の鍵生成手段)により生成された前記第2の鍵を前記情報要求者側へ提供する第2の鍵提供ステップ(第2の鍵提供手段)が構成されている。

【0233】前記第2の鍵生成ステップ(第2の鍵生成

手段)は、前記変換情報(A(+)RN)に対し、前記第2の鍵(I1, I2, …I_n)を用いてのあるアルゴリズム(イクスクリューシブオア)に従った変換処理と前記情報要求者側の秘密鍵(SKU)を用いてのあるアルゴリズム(イクスクリューシブオア)に従った変換処理とを施すことを条件として前記情報(コンテンツA)を再生できるように定められた前記第2の鍵(I1, I2, …I_n)を生成する。

【0234】(4) 前述した本実施の形態では、図21に基づいて説明したように、情報の不正コピーを防止する発明が開示されている。

【0235】この発明は、不正コピーを防止することを目的とし、その目的達成のために、次のような手段を採用した。

【0236】暗号化された暗号情報内に、当該暗号情報を復号化するための鍵情報が埋込まれており、該鍵情報を読出す鍵読出手段(MPEG2、復号化器82、電子透かし検出器83)と、該鍵読出手段より読出された鍵を用いて前記暗号情報を復号化して情報を再生する復号化手段(ICカード65、TV16、パソコン14)とを含み、前記復号化手段は、前記再生された情報をユーザが認識できるように出力する出力装置(TV16、CRT52を有するパソコン14)に内蔵されている。

【0237】(5) ICカード65に、エージェント用知識データばかりでなくユーザエージェント26のプログラム自体も記憶させてもよい。そのように構成した場合には、エージェント用知識データとユーザエージェントのプログラム自体とがユーザに常に携帯されるICカードに記録されることとなるために、エージェント用知識データが他人に覗き見されるおそれが少なくなるとともに、ユーザエージェントを他人に使用される不都合も極力防止することができる。しかも、ユーザが勤務先のオフィス等に設置されているパソコンを利用して自分自身のユーザエージェントを活用したい場合には、携帯しているICカード65をそのパソコンに挿入することにより可能となり、わざわざ自宅のパソコン14からユーザエージェントのプログラムとエージェント用知識データとを送信してもらう必要がなくなる。ICカード65のEEPROM94により、エージェント用知識データを格納するエージェント用知識データ格納手段が構成されている。またICカード65のEEPROM94により、エージェントプログラムを格納するエージェントプログラム格納手段が構成されている。このエージェントプログラム格納手段に格納されているエージェントプログラムは、前記ICカードの所有者のために働くエージェントである。

【0238】図15に示したSXAL/MBALの代わりに、RSA公開鍵暗号方式や楕円曲線暗号方式を用いてもよい。

【0239】無線装置71、72、アンテナ76、77

により、コンテンツ提供者と第三者機関との間で情報の通信を無線系メディアを利用して行なうための無線系メディア利用型情報通信手段が構成されている。

【0240】前記S22, S22a, S22bにより、アクセスしてきたものが、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事を処理するために設立された第三者機関本人であるか否かを認証するための第三者機関認証手段が構成されている。前記S15により、番組の合間に挿入されて放送されてきたコマーシャルメッセージをユーザエージェントが検索したコマーシャルメッセージに取換えて編集するコマーシャルメッセージ編集手段が構成されている。前記S16により、番組の合間に挿入されて放送されてきたコマーシャルメッセージをユーザエージェントが検索したコマーシャルメッセージに切換えて放映する切換放映手段が構成されている。

【0241】前記SA10により、ユーザエージェントの移動先予定を登録しておく移動先予定登録手段が構成されている。前記SA45により、第三者エージェントに出向依頼を行なうための処理を行なう出向依頼処理手段が構成されている。SA49により、ユーザエージェントが前記第三者機関へ移動するための第三者機関移動手段が構成されている。

【0242】SA68～SA72により、ユーザエージェントによる購入手段を行なうための購入手段手段が構成されている。この購入手段手段は、購入手段に対するユーザのデジタル署名を行なうためのデジタル署名手段(SA70, SA71, SA72)を含んでいる。このデジタル署名手段は、購入対象を特定可能なオーダ情報と支払方法を特定可能な支払指示との二重署名を行なう機能を持する。SB20～SB27, SB4～SB31により、前記ユーザのデジタル署名を生成するためのデジタル署名生成手段が構成されている。このデジタル署名生成手段は、前記二重署名を生成する機能を有する。

【0243】前記SA73, SA74により、ユーザエージェントのクローンが既に在駐しているところを避け在駐していないところを探し出してユーザエージェントが移動する移動先選択移動手段が構成されている。SA81～SA83, SA88～SA92により、ユーザエージェントを駐在させて新たなコマーシャルメッセージが制作された場合に当該コマーシャルメッセージに対する評価を行なうユーザエージェント駐在評価手段が構成されている。

【0244】ユーザエージェント等が外国のサイト等に移動する場合には、そのサイトでは、どこかの国のエージェントが移動してきたのかをチェックする必要がある場合がある。人間の場合には外国に行くときにビザ(入国許可書)が必要になるのと同様に、エージェントの場合には、ビザ(入国許可書)に相当するものをチェックして、そのエージェントの侵入を許可するか否かを判断

するのが望ましい。

【0245】そこで、アクセスしてきたエージェントがどこかの国のユーザまたは業者のために働くエージェントであるかをチェックするための国籍証明データを当該エージェントに持たせておく。この国籍証明データは、前述した第三者機関等からなる国籍証明書発行機関が外国に行こうとするエージェントに発行する。国籍証明書発行機関には、当該エージェントの公開鍵や必要に応じて秘密鍵が登録されており、国籍証明書発行機関は、これら公開鍵あるいは秘密鍵を利用して当該エージェントの本人確認を行なった上で、当該エージェントに対し国籍証明書を発行する。そして、当該エージェントが外国のサイトにアクセスしてそのサイトに移動しようとした際に、当該サイト側では、当該エージェントの公開鍵や秘密鍵を利用して当該エージェントの本人確認を行なった上で、当該エージェントが保有している国籍証明書を確認してアクセスを許してよいか否かを判断する。

【0246】一方、国籍証明書の発行の代わりに、当該エージェントが移動しようとする外国に当該エージェントが入国してもよいという入国許可証を当該エージェントに発行してもよい。その場合には、前述と同様に、第三者機関等からなる入国証明書発行機関が、登録されている公開鍵や秘密鍵等を利用して当該エージェントの本人確認を行なった上で、当該エージェントに対し入国証明書を発行する。

【0247】前述したように、ユーザエージェント26等が知識として記憶している公開鍵や秘密鍵を、そのユーザエージェント26のユーザと同じ公開鍵および秘密鍵にした実施の形態を示したが、その代わりに、ユーザの公開鍵や秘密鍵と異なった公開鍵や秘密鍵をユーザエージェント26等に記憶させておいてもよい。そのようにすれば、ユーザエージェント26はデジタル署名等を行なった場合に、後々、ユーザ自身がデジタル署名を行なったのかまたはユーザエージェントがデジタル署名を行なったのかを判別することが可能となる。このように、ユーザとそのエージェントとの鍵を異ならせる場合には、公開鍵あるいは秘密鍵を登録しておく鍵登録機関に、ユーザの公開鍵あるいは秘密鍵とそのエージェントの公開鍵あるいは秘密鍵とを対応づけて登録しておくのが望ましい。

【0248】前述した実施の形態では、第三者エージェントが、依頼された仕事の実行として当事者の一方または双方に違法性あるか否かを監視するものとしたが違法性の有無の関し専門の第三者エージェントがネットワーク上を巡回してパトロールするようにし、その監視用第三者エージェントが訪れたプレース上において、ユーザエージェントや業者側エージェント等をその監視用第三者エージェントが尋問して違法性の有無の監視を行なうようにしてもよい。

【0249】ユーザエージェント等が過去にどこかのサイ

トを訪れてどのような仕事を誰のために実行したか等の、エージェントの過去の仕事履歴データを当該エージェントに記憶させておいてもよい。そのようにすれば、いわゆる契約ネット（contractnet）を利用したタスクの分配に際し、マネージャー側がその仕事履歴データに基づいてどの規約者（エージェント）がタスクの実行に適しているか否かを突き止めることができ、その適している規約者（エージェント）に対して指名落札（directed-award）を行なうことが可能となる。なお、契約ネットとは、多数の処理モードの交渉を通じて問題を分割し、各モードに副問題（これをタスクと呼ぶ）を割当てするためのモデルのことである。

【0250】

【課題を解決するための手段の具体例】コンテンツ提供者7とユーザ、または、CM制作者10とユーザにより、当事者が構成されている。前記SA44、SA47により、当事者の一方または双方が行なうには不向かな中立性を要する特定の仕事が発生したことを判定する特定仕事判定手段が構成されている。第三者機関エージェント29、第三者機関常駐エージェント28により、前記当事者双方に対し中立性を有する第三者エージェントが構成されている。この第三者エージェントは、第三者機関8によって運用管理するエージェントに限定されるものではなく、たとえば前記当事者のエージェントが仕事をするテレスクリプト・エンジン内のプレースと同じプレース上で仕事をしている他のエージェントによりこの第三者エージェントを構成してもよい。

【0251】前記SA45、SA64またはSA49～SA53またはSA60またはSA69、SA70により、前記特定仕事判定手段の判定結果に従って、前記当事者双方に対し中立性を有する第三者エージェントに前記特定の仕事を依頼する仕事依頼手段が構成されている。この仕事依頼手段により依頼された仕事を前記第三者エージェントが代理して実行する（図7、図8に示したフローチャート）。前記第三者機関8により、前記特定の仕事を処理するために設立された第三者機関が構成されている。そして前記第三者エージェント（第三者機関エージェント29、第三者機関常駐エージェント28）は、その第三者機関により運用管理され、前記特定の仕事をを行なうために開発されたエージェントである。

【0252】前記ユーザエージェント26と移動先エージェント27とにより、前記当事者のそれぞれの側のために働く当事者エージェントが構成されている。前記特定仕事判定手段は、前記当事者エージェント同士が協調して動作しているときに、当該当事者エージェントでは自己の立場の方に有利となる利己的動作（たとえば有料コンテンツの不法持ち帰りや有料コンテンツに対する虚偽の評価）を行なうおそれのある場合に前記特定の仕事を発生した旨の判定を行なう。

【0253】前記データベース19により、有料コンテ

ンツを格納しているコンテンツ格納手段が構成されている。コンテンツ提供者7により、前記コンテンツ格納手段内の格納コンテンツを提供するコンテンツ提供者が構成されている。ユーザ宅17に居住しているユーザにより、前記コンテンツ提供者が提供するコンテンツ内に入手したいコンテンツがあるか否かの検索を希望するユーザが構成されている。そして、前記特定仕事判定手段は、前記当事者エージェントのうちのユーザ側エージェント（ユーザエージェント26）が前記コンテンツ格納手段に格納されている前記有料コンテンツの検索を希望した場合（SA43によるYESの判断がなされた場合）に前記特定の仕事が生じたことを判定する。

【0254】さらに、前記第三者エージェントは、依頼された仕事の実行を通して前記当事者の一方または双方に違法性があるか否かを監視する監視機能（SC6、SC18）を有する。

【0255】前記SA43、SA44、SA67、SA58により、当事者の一方または双方が行なうには不向かな中立性を要する特定の仕事が発生したことを判定する特定仕事判定ステップが構成されている。前記SA45、SB1、SB5、SB6、SA49、SA50、SB7～SB9により、前記当事者の双方に対し中立性を有する第三者エージェントを調達する第三者エージェント調達ステップが構成されている。前記SA45、SA46、SA64、SA49～SA53、SA69、SA70、SA60により、前記特定仕事判定ステップにより前記特定の仕事が生じた旨の判定がなされた場合に、前記第三者エージェント調達ステップで調達された第三者エージェントに前記特定の仕事の依頼を行なう仕事依頼ステップが構成されている。そしてその仕事依頼ステップにより依頼された第三者エージェントが依頼された前記特定の仕事を実行する（図7、図8に示したフローチャート）。

【0256】前記テレスクリプト・エンジン22とデータベース23とにより、第三者エージェントを提供するためのエージェント提供装置が構成されている。前記データベース23により、複数種類の第三者エージェントを格納しているエージェント格納手段が構成されている。テレスクリプト・エンジン22により、仕事を当事者エージェントに代わって第三者エージェントにより代理実行してもらいたい旨の依頼があった場合に、代理の対象となる前記当事者エージェントに応じた種類の第三者エージェントを前記エージェント格納手段が格納している前記第三者エージェントの中から検索して提供するエージェント検索提供手段が構成されている。

【0257】ユーザエージェント26によりユーザ側のために働くエージェントであって、ネットワーク上を移動して動作するモバイルエージェントで構成されたユーザ側エージェントが構成されている。コンテンツ提供者7により、前記ユーザの要求に応えるサービス業者が

構成されている。移動先エージェント27により、前記サービス業者側のために働く業者側エージェントが構成されている。第三者機関8のプレース25を有するコンピュータ22aにより、前記ユーザ側エージェントのワーキングエリアとして機能し、秘密の漏洩が防止できる秘密保持用ワーキングエリアが構成されている。

【0258】そして、前記ユーザ側エージェントは、秘密にしたい秘密データ(秘密情報S1)を秘密性が保持できる態様(暗号化した態様)で前記知識として記憶しており、該ユーザ側エージェントが移動して仕事を行なう際に、前記秘密データを使用する必要がある場合に(SA44によりYESの判断がなされた場合に)、前記ユーザ側エージェントは、前記秘密保持用ワーキングエリアに移動し(SA49)、該秘密保持用ワーキングエリア内で前記秘密データの秘密性を解除(SA50, SA51)して前記仕事の実行を可能にする。

【0259】前記ユーザ側エージェントは、前記秘密データを暗号化して保有している(図14参照)。そして、ユーザ側エージェントが前記秘密保持用ワーキングエリアに移動した後前記暗号化された秘密データの復号化再生を可能にする(SA50, SA51)。

【0260】また、前記ユーザ側エージェントは、前記秘密データの復号に用いられる復号鍵(SK1)を保有しておらず、前記秘密保持用ワーキングエリアに移動した後、該秘密保持用ワーキングエリア内に取り寄せた前記復号鍵を用いた前記秘密データの復号を可能にする(SA50, SA51, SC2, SC11, SC12)。

【0261】前記秘密データは、前記ユーザの本人認証のための秘密鍵(SKU)を含んでいる(図14参照)。

【0262】前記CD-ROM68bまたはICカード65により、それぞれに独立の知識を持つエージェント同士が協調的に動作するマルチエージェントシステムに使用され、当事者の一方の側のために働くエージェントプログラムを記録している記録媒体が構成されている。この記録媒体に記録されているプログラムは、コンピュータに、当事者の他方のエージェントと打合せする第1の打合せ手段(SA32, SA45, SA55, SA60, SA62, SA68, SA72)と、前記当事者の双方が行なうには不向きな中立性を要する特定の仕事が生じた場合に、前記当事者双方に対し中立性を有する第三者エージェント(第三者機関常駐エージェント28, 第三者機関エージェント29)と打合せする第2の打合せ手段(SA50, SA51, SA64, SA70)と、前記特定の仕事を前記第三者エージェントに代理実行してもらうのに必要な情報(ユーザのプロフィール情報96等)を当該第三者エージェントに通知する必要情報通知手段(SA64, SA70, SA51)として機能させるためのものである。

【0263】前述した当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事の他の例としては、当事者エージェント同士が対立するというトラブルが発生した場合の仲裁やどちらのエージェントが正しいかの判定、当事者エージェントの一方または双方が本当に正しい当事者のエージェントであるかを立証するための第三者による証明等が考えられる。つまり、この特定の仕事とは、当事者だけでは解決が困難または不可能な中立性を要する仕事すべてを対象とする。

【0264】

【課題を解決するための手段の具体例の効果】請求項1に関しては、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事を当事者双方に対し中立性を有する第三者エージェントが代理して実行してくれるために、中立性を保ちながら特定の仕事の実行が可能となる。

【0265】請求項2に関しては、請求項1に関する効果に加えて、前記第三者エージェントが、前記特定の仕事を処理するために設立された第三者機関により運用管理され、前記特定の仕事をを行なうために開発されたエージェントであるために、当事者にとってより一層中立性のあるエージェントによりより一層中立性のある代理実行が期待できる。

【0266】請求項3に関しては、請求項1または請求項2に関する効果に加えて、当事者エージェントでは自己の立場の方に有利となる利己的動作を行なうおそれのある場合に前記特定の仕事が発生した旨の判定が行なわれ、第三者エージェントによる代理実行が行なわれるために、当事者エージェントによる利己的な動作による不都合を極力防止することができる。

【0267】請求項4に関しては、請求項3に関する効果に加えて、ユーザ側エージェントがコンテンツ格納手段に格納されている有料コンテンツの検索を希望した場合に、特定の仕事が生じたと判定されて第三者エージェントがその特定の仕事を代理実行してくれるために、ユーザ側エージェントが有料コンテンツを検索してその有料コンテンツに対する料金を支払うことなく有料コンテンツを盗んでしまう不都合が極力防止できる。

【0268】請求項5に関しては、請求項1～請求項4のいずれかの効果に加えて、第三者エージェントが、依頼された仕事の実行を通して前記当事者の一方または双方に違法性があるか否かを監視する監視機能を有するために、当事者の一方または双方に違法性があった場合にはそれが監視可能となる。

【0269】請求項6に関しては、仕事を当事者エージェントに代わって第三者エージェントにより代理実行してもらいたい旨の依頼があった場合に、代理の対象となる前記当事者エージェントに応じた種類の第三者エージェントが検索されて提供されるために、当事者エージェントに代わって仕事を代理実行する第三者エージェント

としてその当事者エージェントに似ている適したエージェントを選任することができる。

【0270】請求項7に関しては、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が生じた場合に、当事者の双方に対し中立性を有する第三者エージェントにその特定の仕事を代理実行してもらうことのできるプログラムが記録された記録媒体を提供することができる。

【0271】請求項8に関しては、当事者の一方または双方が行なうには不向きな中立性を要する特定の仕事が生じた場合に、当事者の双方に対し中立性を有する第三者エージェントが調達されてその第三者エージェントに前記特定の仕事を代理実行してもらうことができる。

【0272】請求項9に関しては、モバイルエージェントで構成されているユーザ側エージェントがネットワーク上を移動して仕事を行なうに際し、ユーザ側エージェントが秘密データを使用する必要がある場合には、ユーザ側エージェントが秘密保持用ワーキングエリアに移動してそこで秘密データの秘密性を解除して前記仕事の実行が可能となり、秘密データの漏洩を防止できながらその秘密データを使用しての仕事の実行が可能となる。

【0273】請求項10に関しては、請求項9に関する効果に加えて、ユーザ側エージェントが前記秘密データを暗号化して保有しているために、ユーザ側エージェントがネットワーク上を移動して動作したとしてもその秘密データが他人に漏洩されることを極力防止することができる。

【0274】請求項11に関しては、請求項10に関する効果に加えて、前記秘密データの復号に用いられる復号鍵をユーザ側エージェントが保有していないために、ユーザ側エージェントがネット上を移動して動作した際に前記暗号化された秘密データが他人に知られたとしても、それを復号するための復号鍵までは他人に知られることが防止できるために、前記秘密データの漏洩をより確実に防止することができる。

【0275】請求項12に関しては、請求項9～請求項11に関する効果に加えて、ユーザ側エージェントが保有している秘密データは、前記ユーザの本人認証のための秘密鍵を含んでいるために、前記秘密保持用ワーキングエリア内に移動することによりその秘密鍵を用いてのユーザの本人認証を行なうことが可能となり、ユーザ側エージェントにより一層高度なユーザの代理仕事を行なわせることが可能となる。

【図面の簡単な説明】

【図1】情報の検索および配信を説明するための説明図である。

【図2】各種エージェントの動作を説明するための説明図である。

【図3】パソコンの制御動作を示すフローチャートである。

【図4】ユーザエージェントの動作を示すフローチャートである。

【図5】ユーザエージェントの動作を示すフローチャートである。

【図6】ユーザエージェントの動作を示すフローチャートである。

【図7】第三者機関常駐エージェントの動作を示すフローチャートである。

【図8】第三者機関エージェントの動作を示すフローチャートである。

【図9】CMの検索を行なうためのエージェントの動作を説明するための説明図である。

【図10】ユーザエージェントの動作を示すフローチャートである。

【図11】(a)はCMプレース常駐エージェントの動作を示すフローチャートであり、(b)はCM制作者の情報処理コンピュータの制御動作を示すフローチャートである。

【図12】ユーザのパソコンのCRTにより表示されたコマースメッセージの表示画面図である。

【図13】コンテンツ提供者の通信装置とユーザのパソコンとの制御回路を示すブロック図である。

【図14】ユーザのICカードの制御回路および記録情報を示すブロック図である。

【図15】暗号方式SXAL/MBALの概要説明図である。

【図16】コンテンツ提供者の通信装置の制御動作を示すフローチャートである。

【図17】ユーザのパソコンの制御動作を示すフローチャートである。

【図18】ユーザ認証処理の制御動作を示すフローチャートである。

【図19】コンテンツの不正コピーを防止するための制御回路を示すブロック図である。

【図20】情報の検索および配信の他の例を示す説明図である。

【図21】コンテンツの不正コピーを防止するための他の例を示すブロック図である。

【図22】通信装置の制御動作の他の例を示すフローチャートである。

【図23】ユーザ認証処理の他の例を示すフローチャートである。

【図24】ユーザのパソコンの制御動作の他の例を示すフローチャートである。

【符号の説明】

1は衛星

2は放送局

10はCM制作者

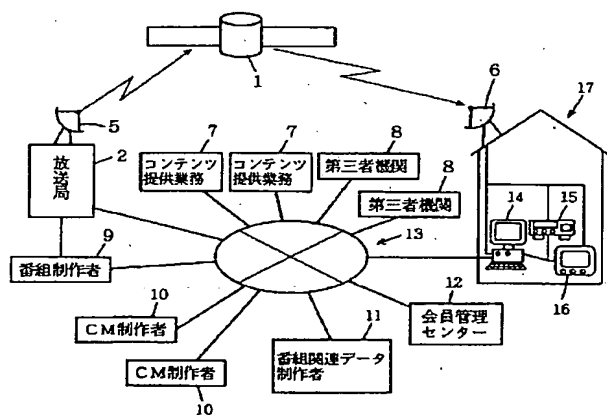
11は番組関連データ制作者

7はコンテンツ提供者

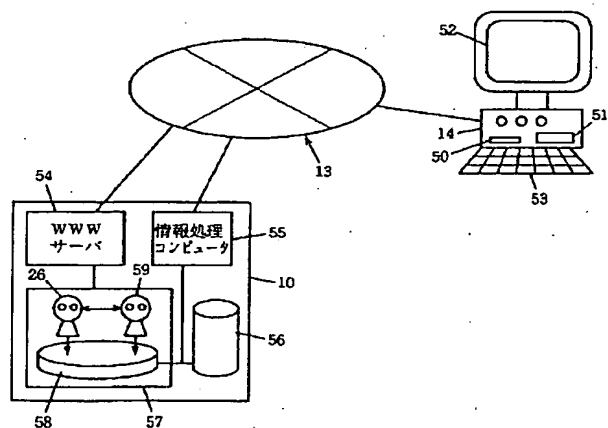
59

- 8 は第三者機関
 14 はパソコン
 16 はTV
 15 はVTR
 13 はインターネット
 26 はユーザエージェント
 27 は移動先エージェント
 28 は第三者機関常駐エージェント
 29 は第三者機関エージェント
 19, 23, 56, 70 はデータベース
 52 はCRT
 50 はICカード挿入口

【 図1 】



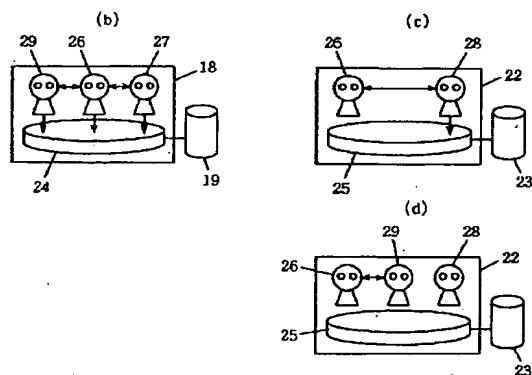
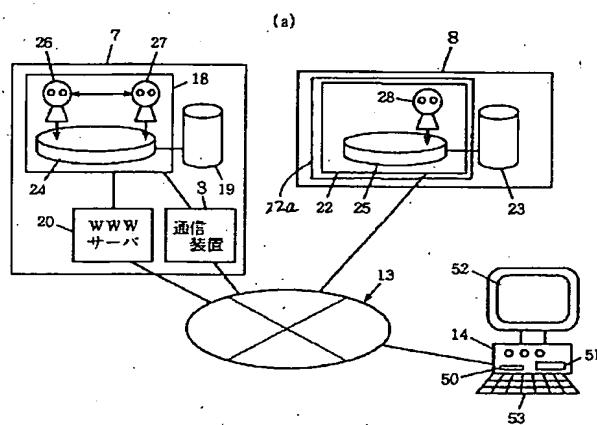
【 図9 】



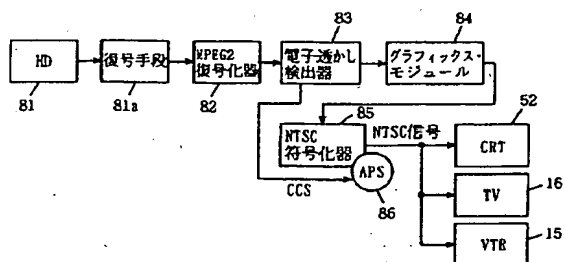
60

- 18, 22, 57 はテレクリプト・エンジン
 24, 25, 58 はプレス
 3 は通信装置
 59 は常駐エージェント
 69 は管理サーバー
 68b はCD-ROM
 65 はICカード
 96 はプロフィール情報
 82 はMP E G 2 復号化器
 83 は電子透かし検出器
 86 はAPS

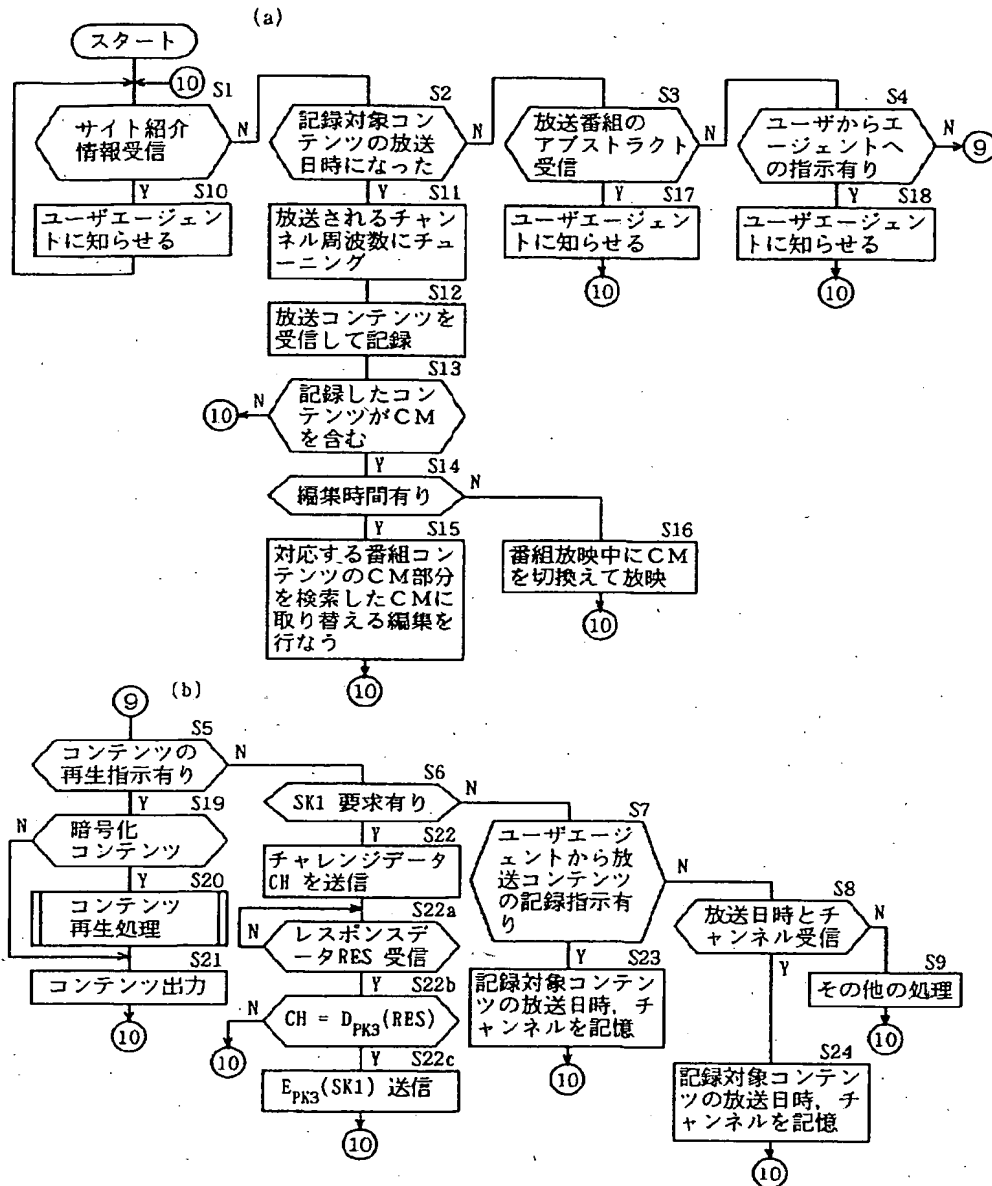
【 図2 】



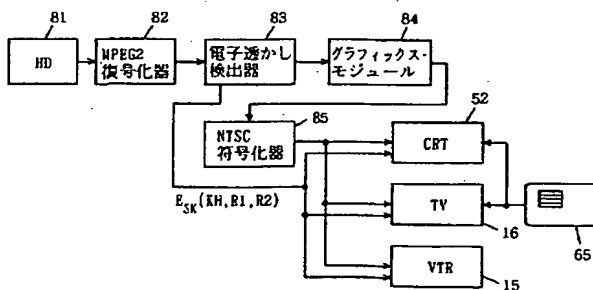
【 図19 】



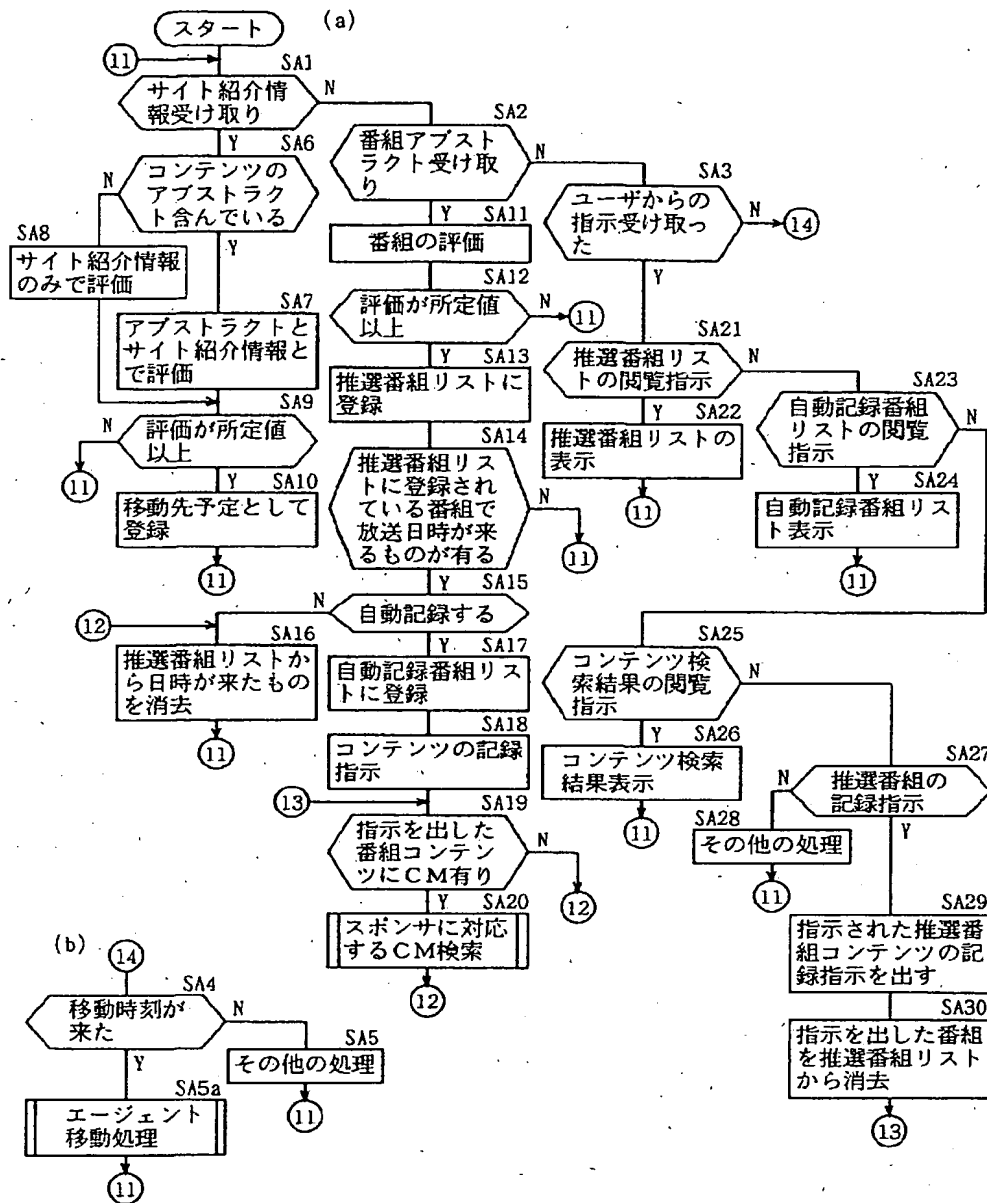
【 図3 】



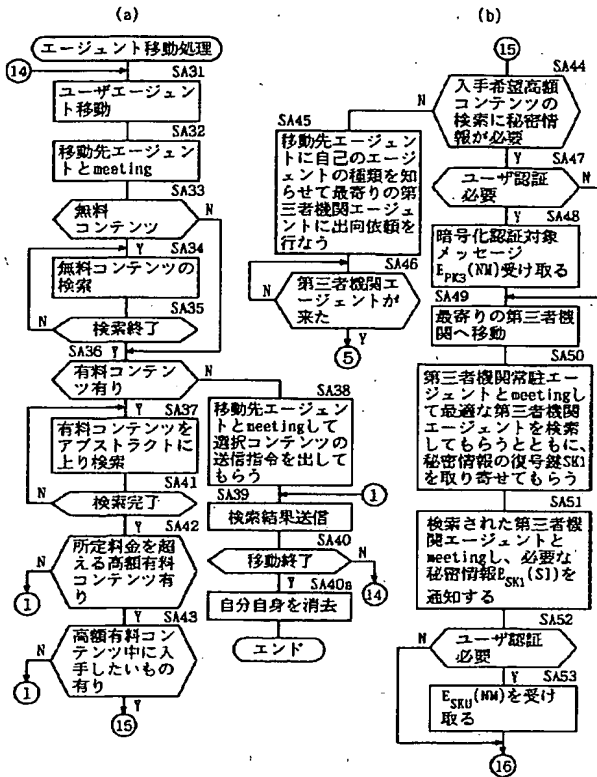
【 図21 】



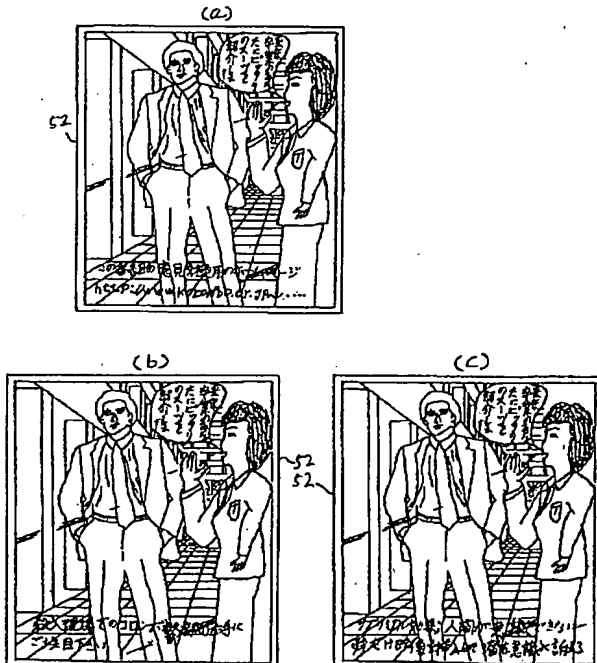
【 図4 】



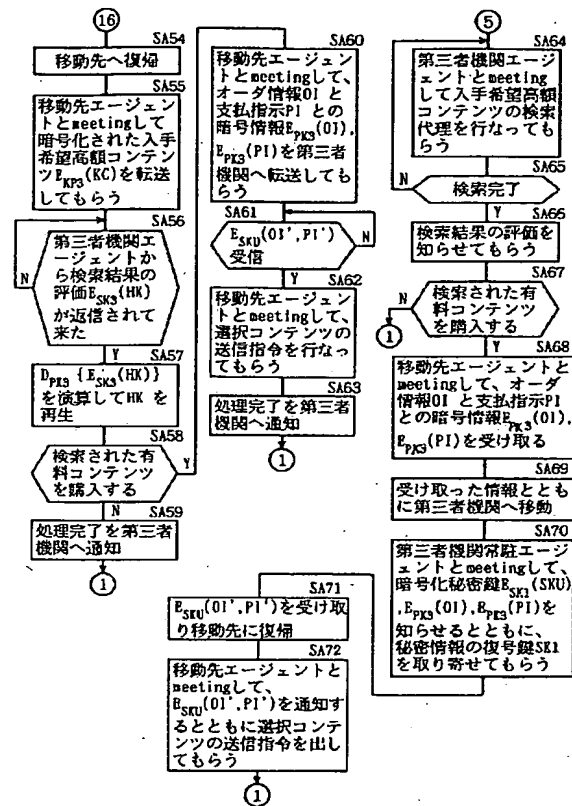
【 図5 】



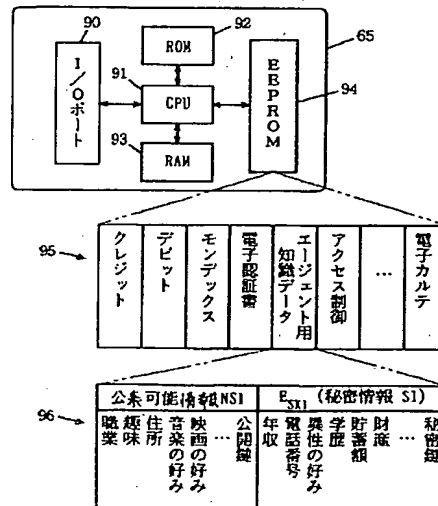
【 図1 2 】



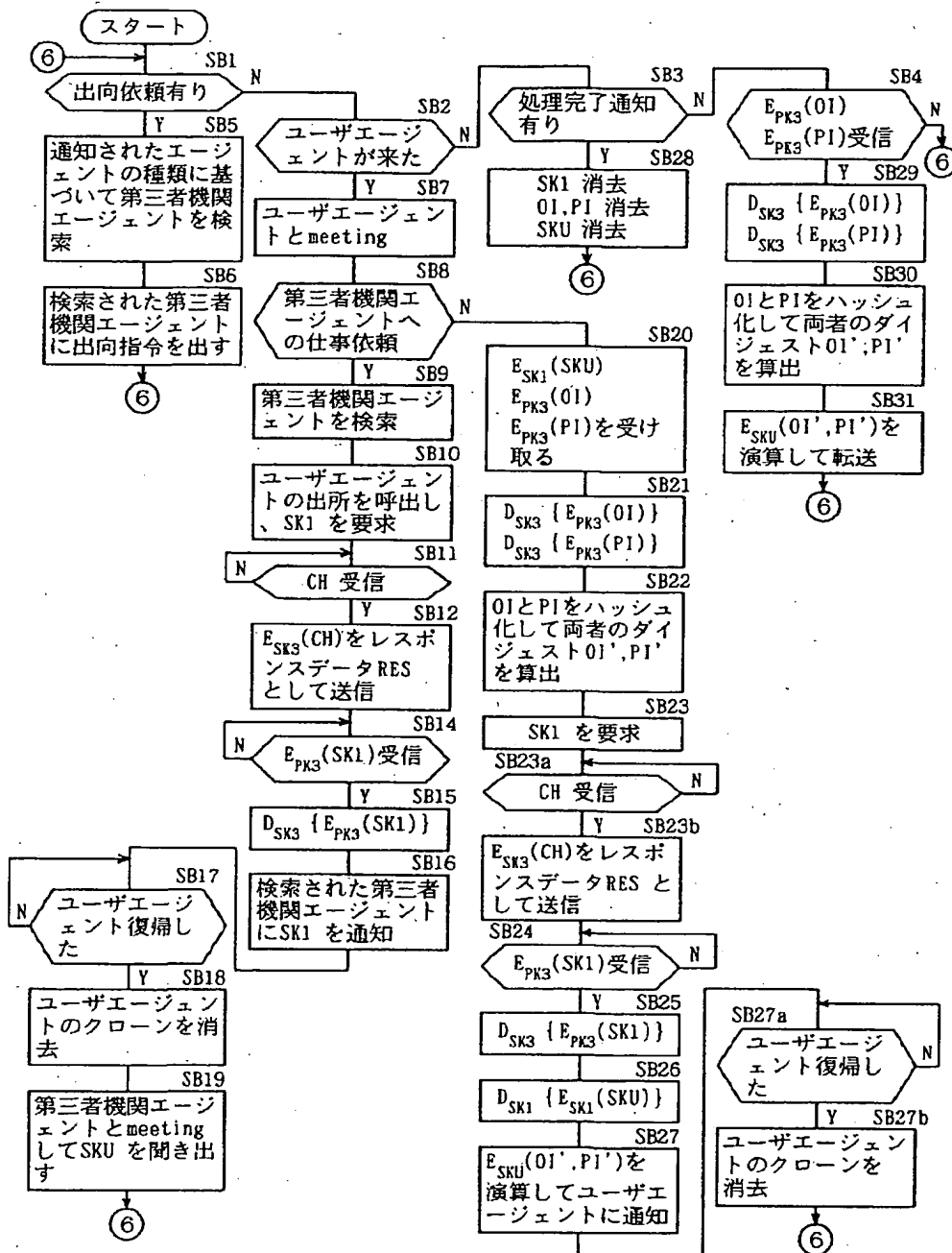
【 図6 】



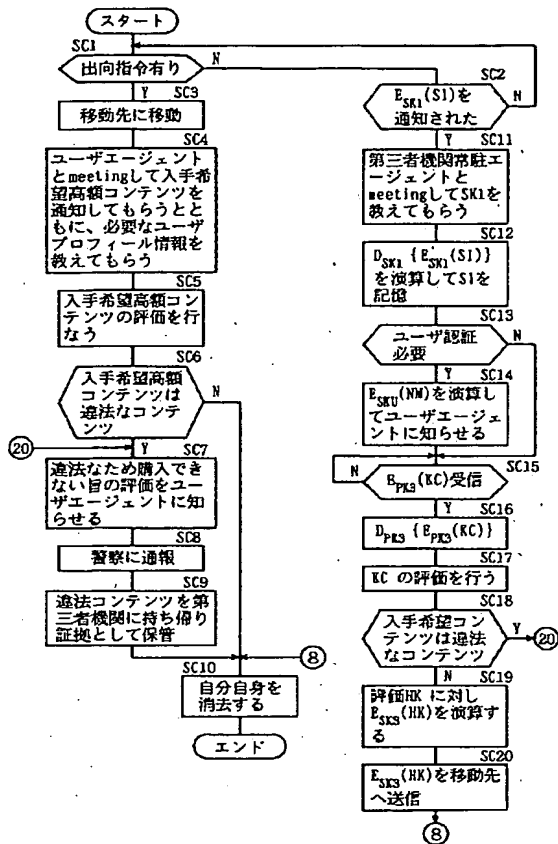
【 図1 4 】



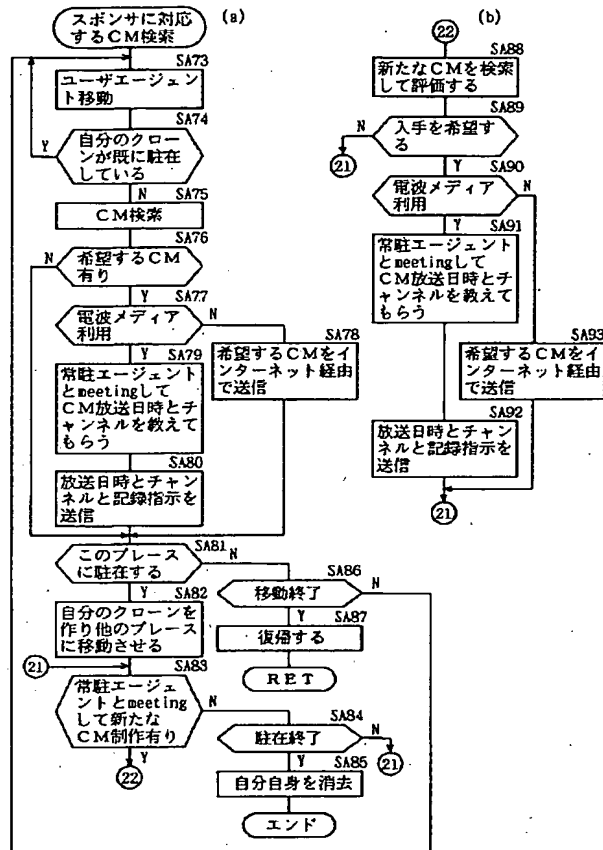
【 図7 】



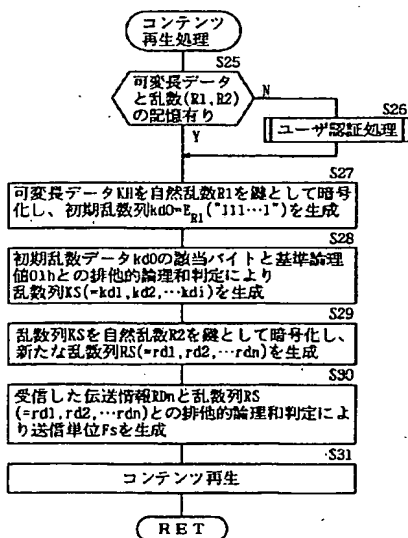
【 図 8 】



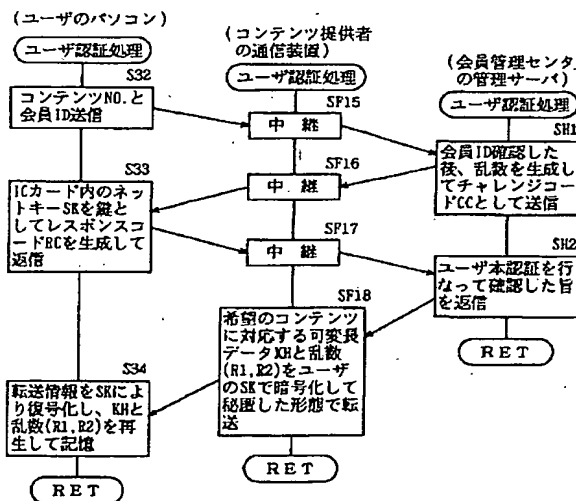
【 図 10 】



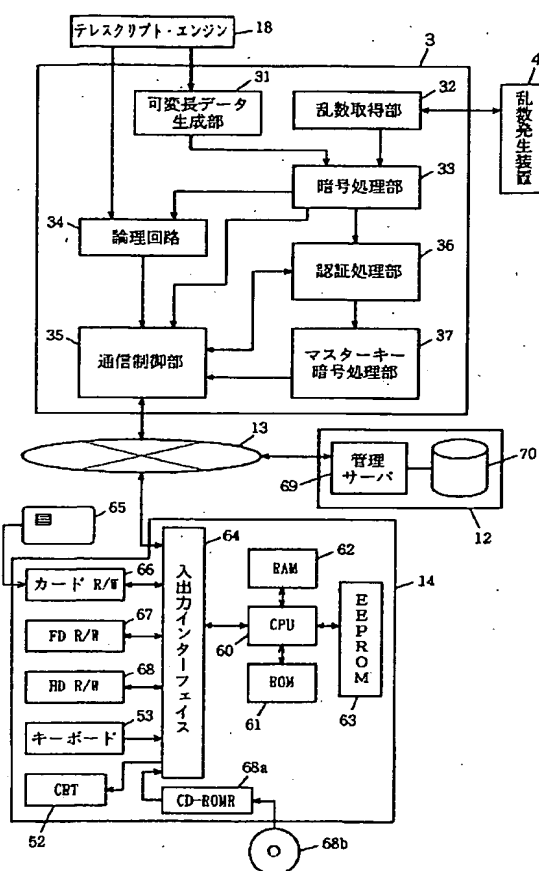
【 図 17 】



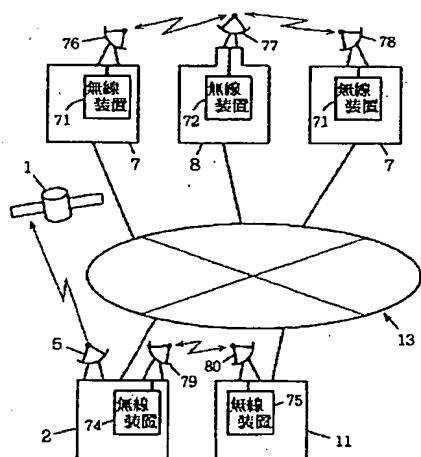
【 図 18 】



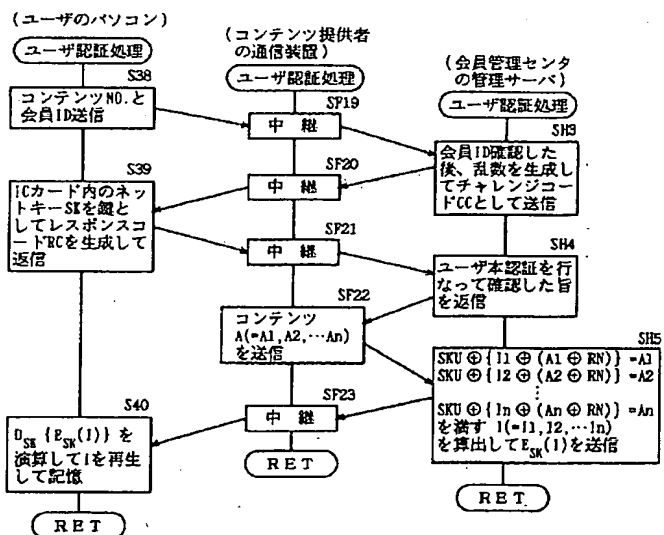
【 図 1 3 】



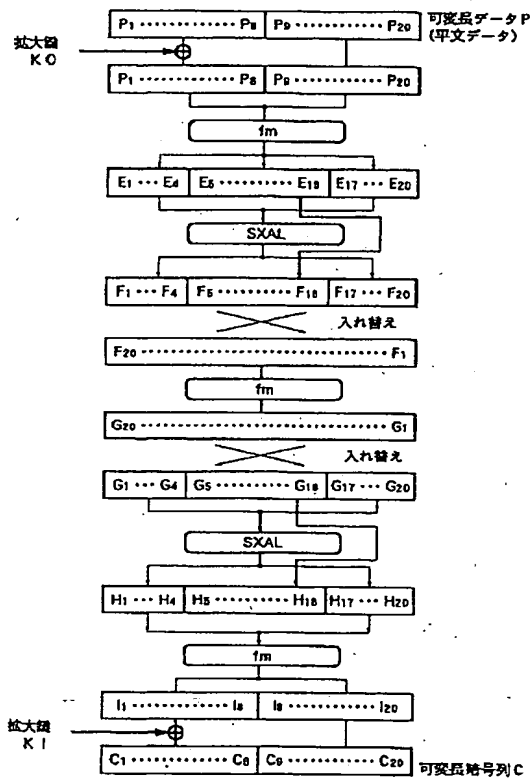
【 図 2 0 】



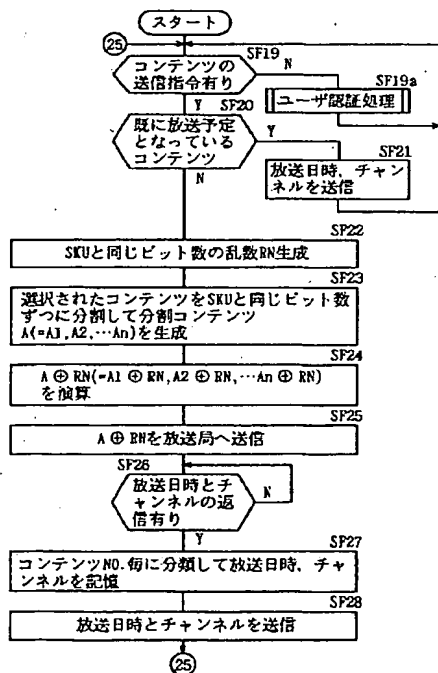
【 図 2 3' 】



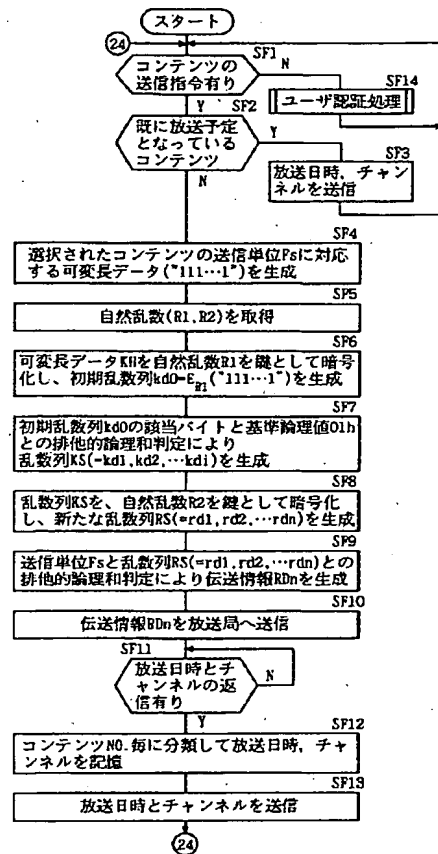
【 図15 】



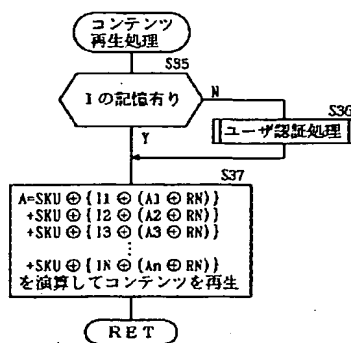
【 図22 】



【 図16 】



【 図24 】



フロント ページの続き

(72)発明者 藤井 幹雄

神奈川県横浜市青葉区美しが丘5 丁目35番
地の2 株式会社ローレルインテリ ジェン
ト システムズ内

(72)発明者 塚本 豊

神奈川県横浜市青葉区美しが丘5 丁目35番
地の2 株式会社ローレルインテリ ジェン
ト システムズ内